ProtectTools
ユーザ ガイド

初版：2007 年 5 月

製品番号：451271-291

目次

1 セキュリティの概要

HP ProtectTools セキュリティ マネージャ ソフトウェアは、コンピュータ本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立つセキュリティ機能を提供します。以下のソフトウェア モジュールによって、高度なセキュリティ機能が提供されます。

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools

コンピュータで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。たとえば、Embedded Security for HP ProtectTools は、TPM（Trusted Platform Module）セキュリティ チップが内蔵されているコンピュータでのみ使用できます。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。詳しくは、http://www.hp.com/jp/を参照してください。

注記： このガイドの操作手順は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

HP ProtectTools の機能

次の表で、HP ProtectTools モジュールの主な機能を詳しく説明します。

モジュール	主な機能
Credential Manager for HP ProtectTools	● Credential Manager には、個人のパスワードを保管できます ● シングルサインオンは、パスワードで保護されたさまざまな Web サイト、アプリケーション、およびネットワーク リソース用の複数のパスワードを記憶します ● シングルサインオンは、ユーザ認証に Java™カードや指紋認証などの異なるセキュリティ テクノロジの組み合わせを要求することによって、さらなる保護機能を提供します ● パスワード記憶域は暗号化によって保護されており、TPM 内蔵セキュリティ チップ、または Java カードや指紋認証などのセキュリティ デバイス認証を使用することによって強化できます
Embedded Security for HP ProtectTools	● Embedded Security は、TPM（Trusted Platform Module）内蔵セキュリティ チップを使用して、コンピュータ本体に保存されている機密のユーザ データまたは証明情報を不正なアクセスから保護するために役立ちます ● Embedded Security を使用すると、ユーザ データを保護するための PSD（Personal Secure Drive）を作成できます ● Embedded Security は、保護されたデジタル証明情報の操作のための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）をサポートします
Java Card Security for HP ProtectTools	● Java Card Security は、オペレーティング システムがロードされる前のユーザ認証を行うために、HP ProtectTools Java Card を設定します ● Java Card Security では、管理者とユーザの Java Card を個別に設定します
BIOS Configuration for HP ProtectTools	● BIOS Configuration を使用すると、電源投入時のユーザおよび管理者パスワードの管理機能にアクセスできます ● BIOS Configuration は、F10 セットアップと呼ばれる、ブート前 BIOS コンフィギュレーション ユーティリティの代わりに使用できます。 ● DriveLock は、ハードディスク ドライブがシステムから取り外されている場合でも、ハードディスク ドライブを不正なアクセスから保護できます。ユーザは追加のパスワードを記憶する必要がありません。
Drive Encryption for HP ProtectTools	● Drive Encryption では、ボリューム全体にわたる完全なハードディスク ドライブ暗号化が可能です ● Drive Encryption では、データの暗号化解除やデータへのアクセスにブート前認証が強制されます

HP ProtectTools セキュリティへのアクセス

Windows®の[コントロール パネル]から HP ProtectTools セキュリティにアクセスするには、次の操作を行います。

▲ **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

注記： Credential Manager モジュールを設定した後は、Windows のログオン画面から直接 Credential Manager にログオンして HP ProtectTools を起動することもできます。詳しくは、17 ページの「Credential Manager を使用した Windows へのログオン」を参照してください。

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することにより、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題に対処するためのソリューションを提供できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成

盗難からの保護

盗難の例として、職場や公共の場での、機密データや顧客情報を含むコンピュータの盗難が挙げられます。盗難からの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の項目を参照してください。
  - 48 ページの 「スマート カードの電源投入時認証サポートの有効/無効の設定」
  - 49 ページの 「内蔵セキュリティの電源投入時認証サポートの有効/無効の設定」
  - 41 ページの 「Java Card への名前の割り当て」
  - 54 ページの 「Drive Encryption for HP ProtectTools」
- DriveLock（ドライブロック）は、ハードディスク ドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。50 ページの 「DriveLock によるハードディスク ドライブ保護の有効/無効の設定」を参照してください。
- Embedded Security for HP ProtectTools モジュールで提供される Personal Secure Drive 機能では、機密データを暗号化して、認証なしではアクセスできないようにします。以下の項目を参照してください。
  - 30 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
  - 33 ページの 「Personal Secure Drive（PSD）の使用」

機密データへのアクセス制限

契約検査官がオンサイトで作業しており、機密の財務データの確認のためにコンピュータへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

- DriveLock は、ハードディスク ドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。50 ページの 「DriveLock によるハードディスク ドライブ保護の有効/無効の設定」を参照してください。

内部または外部からの不正なアクセスの防止

機密データや顧客情報を含むコンピュータが内部または外部からアクセスされると、不正なユーザが社内ネットワーク リソースに侵入したり、金融サービス、役員、または研究開発チームからのデー

タ、または患者記録や個人の財務データなどの個人情報を入手したりできてしまう可能性があります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の項目を参照してください。
  - 48 ページの 「スマート カードの電源投入時認証サポートの有効/無効の設定」
  - 49 ページの 「内蔵セキュリティの電源投入時認証サポートの有効/無効の設定」
  - 41 ページの 「Java Card への名前の割り当て」
  - 54 ページの 「Drive Encryption for HP ProtectTools」
- Embedded Security for HP ProtectTools は、以下の方法で、コンピュータ本体に保存されている機密のユーザ データまたは証明情報を保護するために役立ちます。
  - 30 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
  - 33 ページの 「Personal Secure Drive（PSD）の使用」
- Credential Manager for HP ProtectTools は、以下方法で、不正なユーザがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにするために役立ちます。
  - 12 ページの 「セットアップ手順」（Credential Manager のセットアップ）
  - 18 ページの 「シングルサインオンの使用」
- Personal Secure Drive 機能では、以下の方法で機密データを暗号化し、認証なしではアクセスできないようにします。
  - 30 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
  - 33 ページの 「Personal Secure Drive（PSD）の使用」

強力なパスワード ポリシーの作成

いくつもの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合、Credential Manager for HP ProtectTools で以下の方法により、パスワードやシングルサインオンのための保護されたリポジトリが提供されます。

- 12 ページの 「セットアップ手順」（Credential Manager のセットアップ）
- 18 ページの 「シングルサインオンの使用」

セキュリティを強化するために、Embedded Security for HP ProtectTools は次に、ユーザ名とパスワードのリポジトリを保護します。これにより、ユーザはメモに残したり覚えたりしなくても、複数の強力なパスワードを保持することができます。30 ページの 「セットアップ手順」（Embedded Security のセットアップ）を参照してください。

その他のセキュリティ対策

セキュリティの役割の割り当て

コンピュータのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザに割り当てることが、重要な作業の 1 つです。

注記：　小さな組織や個人で使用する場合などは、一人の人がすべての役割を受け持つこともできます。

HP ProtectTools では、セキュリティの責任および権限を以下のように分けられます。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Java™ Cards、指紋認証システム、USB トークンなど、配備するセキュリティ機能を決定します。

  注記：　HP ProtectTools の機能の多くは、セキュリティ統括責任者が HP と協力してカスタマイズできます。詳しくは、HP の Web サイト http://www.hp.com/jp/を参照してください。

- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ統括責任者が Java Card の配備を決定した場合、IT 管理者は Java Card の BIOS セキュリティ モードを有効にすることができます。
- ユーザ：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムで Java Card を有効にしている場合、ユーザは Java Card の PIN を設定し、そのカードを認証に使用できます。

HP ProtectTools のパスワードの管理

HP ProtectTools セキュリティ マネージャの機能のほとんどは、パスワードによってセキュリティ保護されています。次の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者だけが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザまたは管理者が設定できます。

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
Credential Manager のログオン パスワード	Credential Manager	このパスワードには、次の 2 つのオプションがあります ● Windows にログオンした後、Credential Manager にアクセスするための別のログオンで使用できます ● Windows ログオン プロセスの代わりに使用し、Windows と Credential Manager に同時にアクセスできます
Credential Manager リカバリ ファイルのパスワード	Credential Manager、IT 管理者が設定	Credential Manager リカバリ ファイルへのアクセスを保護します
基本ユーザ キーのパスワード 注記：　内蔵セキュリティ パスワードとも呼ばれます	Embedded Security	安全な電子メール、ファイル、およびフォルダの暗号化など Embedded Security 機能へのアクセスに使用します。電源投入時認証に使用すると、コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータを保護します
緊急リカバリ トークンのパスワード	Embedded Security、IT 管理者が設定	内蔵セキュリティ チップ用のバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
注記： 緊急リカバリ トークン キーのパスワードとも呼ばれます		
所有者のパスワード	Embedded Security、IT 管理者が設定	システムと TPM チップを、Embedded Security のすべての所有者機能への不正なアクセスから保護します
Java™ Card の PIN	Java Card Security	Java Card の内容へのアクセスを保護し、Java Card のユーザを認証します。電源投入時認証に使用すると、Java Card の PIN の入力により[Computer Setup]ユーティリティおよびコンピュータのデータも保護されます Java Card トークンが選択されている場合は、Drive Encryption のユーザを認証します
[Computer Setup]のパスワード **注記：** BIOS の管理者パスワード、F10 セットアップ パスワード、またはセキュリティ セットアップ パスワードとも呼ばれます	BIOS Configuration、IT 管理者が設定	[Computer Setup]ユーティリティへのアクセスを保護します
Power-on Password（電源投入時パスワード）	BIOS Configuration	コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータを保護します
Windows のログオン パスワード	Windows の[コントロール パネル]	手動ログオンで使用するか、または Java Card に保存できます

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成し、そのパスワードが危険にさらされないようにするために、以下のガイドラインを考慮してください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は常に、半角アルファベットと半角数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの I または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分割します。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字をその次の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピュータのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピュータ上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

HP ProtectTools Backup and Restore

HP ProtectTools Backup and Restore には、サポートされているすべての HP ProtectTools モジュールからの証明情報をバックアップおよび復元するための便利で、すばやく実行できる機能が用意されています。

証明情報および設定のバックアップ

以下の方法で証明情報をバックアップできます。

- [HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）を使用して、HP ProtectTools モジュールの選択とバックアップを行う
- 事前に選択された HP ProtectTools モジュールをバックアップする

  注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

- バックアップのスケジュールを設定する

  注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

[HP ProtectTools Backup Wizard]を使用した HP ProtectTools モジュールの選択とバックアップ

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Backup Options]**（バックアップ オプション）をクリックします。[HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）が起動します。画面の説明に沿って操作し、証明情報をバックアップします。

バックアップ オプションの設定

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Backup Options]**（バックアップ オプション）をクリックします。[HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。
5. **[Storage File Password]**（ストレージ ファイルのパスワード）を設定および確認したら、**[Remember all passwords and authentication values for future automated backups]**（将来の自動バックアップのすべてのパスワードと認証値を記憶する）を選択します。
6. **[Save Settings]**（設定の保存）→**[Finish]**（完了）の順にクリックします。

事前に選択された HP ProtectTools モジュールのバックアップ

注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Backup]**をクリックします。

バックアップ スケジュールの設定

注記： この方法を使用するには、バックアップ オプションを設定する必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[HP ProtectTools]→[Backup and Restore]**（バックアップおよび復元）の順にクリックします。
3. 右側のパネルで、**[Schedule Backups]**（バックアップ スケジュールの設定）をクリックします。
4. **[Task]**（タスク）タブで、**[Enable]**（有効）チェック ボックスにチェックを入れて、スケジュールされたバックアップを有効にします。
5. **[Set Password]**（パスワードの設定）をクリックし、**[Set Password]**（パスワードの設定）ダイアログ ボックスでパスワードを入力して確認します。**[OK]**をクリックします。

6. **[Apply]**（適用）をクリックします。**[Schedule]**（スケジュール）タブをクリックします。**[Schedule Task]**（タスクのスケジュール）の矢印をクリックし、自動バックアップの頻度を選択します。

7. **[Start time]**（開始時刻）の下で、**[Start time]**（開始時刻）の矢印を使用して、バックアップ開始の正確な時刻を選択します。

8. **[Advanced]**（詳細）をクリックして、開始日、終了日、および繰り返しタスクの設定を選択します。**[Apply]**（適用）をクリックします。

9. **[Settings]**（設定）をクリックし、**[Scheduled Task Completed]**（スケジュールされたタスクの完了）、**[Idle Time]**（アイドル時間）、および**[Power Management]**（電源管理）の設定を選択します。

10. **[Apply]**（適用）をクリックし、**[OK]**をクリックしてダイアログ ボックスを閉じます。

証明情報の復元

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[HP ProtectTools]**→**[Backup and Restore]**（バックアップおよび復元）の順にクリックします。

3. 右側のパネルで、**[Restore]**（復元）をクリックします。[HP ProtectTools Restore Wizard]（HP ProtectTools 復元ウィザード）が起動します。画面に表示される説明に沿って操作します。

設定の選択

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。

2. 左側のパネルで、**[HP ProtectTools]**→**[Settings]**（設定）の順にクリックします。

3. 右側のパネルで、設定を選択して**[OK]**をクリックします。

2 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools では、次のセキュリティ機能を使用して、コンピュータを不正なアクセスから保護します。

- Windows へのログオン時のパスワードに代わる、Java Card や指紋認証システムなどを使用した Windows へのログオン。詳しくは、13 ページの 「証明情報の登録」を参照してください。
- Web サイト、アプリケーション、および保護されたネットワーク リソースでの証明情報を自動的に記憶するシングルサインオン機能。
- Java Card や指紋認証システムなどの、オプションのセキュリティ デバイスのサポート。
- コンピュータのロック解除にはオプションのセキュリティ デバイスを使用した認証を必要とするなどの、追加のセキュリティ設定のサポート。

セットアップ手順

Credential Manager へのログオン

設定に応じて、以下のどれかの方法で Credential Manager にログオンできます。

- [Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）（推奨）
- 通知領域の[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコン
- HP ProtectTools セキュリティ マネージャ

注記： Windows のログオン画面の Credential Manager ログオン入力領域から Credential Manager にログオンすると、同時に Windows にもログオンします。

最初に Credential Manager を起動するときは、通常の Windows ログオン パスワードでログオンします。その後、Credential Manager アカウントが、Windows のログオン証明情報を使用して自動的に作成されます。

Credential Manager にログオンした後、指紋や Java Card などの追加の証明情報を登録できます。詳しくは、13 ページの 「証明情報の登録」を参照してください。

次回のログオン時には、ログオン ポリシーを選択して、登録された証明情報の任意の組み合わせを使用することができます。

[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）の使用

[Credential Manager Logon Wizard]を使用して Credential Manager にログオンするには、以下の手順で操作します。

1. 以下のどれかの方法で[Credential Manager Logon Wizard]を起動します。
   - Windows のログオン画面を使用する
   - 通知領域から、**[HP ProtectTools Security Manager]**アイコンをダブルクリックする
   - ProtectTools セキュリティ マネージャの[Credential Manager]（証明情報マネージャ）ページから、ウィンドウの右上隅にある**[Log On]**（ログオン）リンクをクリックする
2. 画面の説明に沿って操作し、Credential Manager にログオンします。

最初のログオン

開始する前に、管理者アカウントで Windows にログオンし、Credential Manager にログオンしていないことが必要です。

1. 通知領域内の[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンをダブルクリックして、HP ProtectTools セキュリティ マネージャを起動します。[HP ProtectTools Security Manager]ウィンドウが開きます。
2. 左側のパネルで**[Credential Manager]**（証明情報マネージャ）をクリックしてから、右側のパネルの右上隅にある**[Log On]**（ログオン）をクリックします。[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）が起動します。
3. **[Password]**（パスワード）ボックスに Windows パスワードを入力して**[Next]**（次へ）をクリックします。

証明情報の登録

[My Identity]（個人 ID）ページを使用して、各種の認証方法、または証明情報を登録できます。登録が完了した後、それらの方法を使用して Credential Manager にログオンできます。

指紋の登録

指紋認証システムでは、Windows パスワードではなく、指紋を使用して認証することで Windows にログオンできます。

指紋認証システムのセットアップ

1. Credential Manager にログオンしたら、指紋認証システムの指紋読み取り装置に指を押し当てます。[Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
2. 画面の説明に沿って操作し、指紋の登録と指紋認証システムのセットアップを完了します。
3. 別の Windows ユーザ用の指紋を登録するには、そのユーザとして Windows にログオンして手順 1 と 2 を繰り返します。

登録された指紋を使用した Windows へのログオン

1. 指紋を登録したらすぐに Windows を再起動します。
2. Windows の[ようこそ]画面で、登録された指のどれかを押し当てて Windows にログオンします。

Java Card、USB eToken、または仮想トークンの登録

注記： この手順を実行するには、カード リーダーまたはスマート カード キーボードを設定しておく必要があります。スマート カードを使用しない場合は、「15 ページの 「仮想トークンの作成」」の説明に沿って仮想トークンを登録できます。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）をクリックします。[Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

USB eToken の登録

1. USB eToken ドライバがインストールされていることを確認します。

   注記： 詳しくは、USB eToken の取扱説明書を参照してください。

2. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
3. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
4. 右側のパネルで、**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）をクリックします。[Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
5. 画面に表示される説明に沿って操作します。

その他の証明情報の登録

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Register Credentials]**（証明情報の登録）をクリックします。[Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

一般的なタスク

Credential Manager の[My Identity]（個人 ID）ページには、すべてのユーザがアクセスできます。[My Identity]ページから、次のことができます。

- 仮想トークンの作成
- Windows ログオン パスワードの変更
- トークン PIN の管理
- ID の管理
- コンピュータのロック

注記： このオプションは、Credential Manager のクラシック ログオン画面が有効に設定されている場合にのみ利用できます。26 ページの 「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

仮想トークンの作成

仮想トークンの機能は、Java Card や USB eToken とよく似ています。このトークンは、コンピュータのハードディスク ドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

新しい仮想トークンを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Virtual Token]**（仮想トークン）をクリックします。[Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。

   注記： **[Virtual Token]**（仮想トークン）オプションがない場合は、14 ページの 「その他の証明情報の登録」の手順を実行します。

4. 画面に表示される説明に沿って操作します。

Windows ログオン パスワードの変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Change Windows Password]**（Windows パスワードの変更）をクリックします。
4. **[Old password]**（古いパスワード）ボックスに、古いパスワードを入力します。
5. **[New Password]**（新しいパスワード）ボックスおよび**[Confirm password]**（パスワードの確認）ボックスに新しいパスワードを入力します。
6. **[Finish]**（完了）をクリックします。

トークン PIN の変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Change Token PIN]**（トークン PIN の変更）をクリックします。
4. PIN を変更するトークンを選択して**[Next]**（次へ）をクリックします。
5. 画面の説明に沿って操作し、PIN の変更を完了します。

ID の管理

システムからの ID の消去

注記： この操作は、Windows ユーザ アカウントには影響しません。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Clear Identity for this Account]**（このアカウントの ID の消去）をクリックします。
4. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。ID がログオフされ、システムから削除されます。

コンピュータのロック

この機能は、Credential Manager を使用して Windows にログオンした場合に利用できます。席を離れている間のコンピュータの安全を確保するには、作業環境のロック機能を使用します。これにより、不正なユーザによるコンピュータへのアクセスを防ぐことができます。このロックは、自分自身と、コンピュータ上の管理者グループのメンバのみが解除できます。

注記： このオプションは、Credential Manager のクラシック ログオン画面が有効に設定されている場合にのみ利用できます。26 ページの 「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

コンピュータのロック解除に Java Card、指紋認証システム、またはトークンが必要となるように作業環境のロック機能を設定することで、セキュリティを強化できます。詳しくは、26 ページの「Credential Manager の設定」を参照してください。

コンピュータをロックするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
3. 右側のパネルで、**[Lock Workstation]**（作業環境をロック）をクリックします。Windows のログオン画面が表示されます。コンピュータのロックを解除するには、Windows パスワードまたは[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）を使用する必要があります。

Windows のログオンの使用

ローカル コンピュータまたはネットワーク ドメインのどちらでも、Credential Manager を使用して Windows にログオンできます。初めて Credential Manager にログオンすると、ローカルの Windows ユーザ アカウントが Windows ログオン サービス用のアカウントとして自動的に追加されます。

Credential Manager を使用した Windows へのログオン

Credential Manager を使用して、Windows のネットワークまたはローカル アカウントにログオンできます。

1. Windows へのログオン用に指紋を登録してある場合は、指を押し当ててログオンします。
2. Windows へのログオン用に指紋を登録していない場合は、画面の左上隅にある指紋アイコンの隣のキーボード アイコンをクリックします。[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）が起動します。
3. **[User name]**（ユーザ名）の矢印→自分の名前の順にクリックします。
4. **[Password]**（パスワード）ボックスにパスワードを入力して**[Next]**（次へ）をクリックします。
5. **[More]**（詳細）→**[Wizard Options]**（ウィザード オプション）の順に選択します。
    a. 次回コンピュータにログオンした時にこの名前を初期設定のユーザ名にする場合は、**[Use last user name on next logon]**（前回のユーザ名を次のログオン時に使用）チェック ボックスにチェックを入れます。
    b. このログオン ポリシーを初期設定の認証方法にする場合は、**[Use last policy on next logon]**（前回のポリシーを次のログオン時に使用）チェック ボックスにチェックを入れます。
6. 画面に表示される説明に沿って操作します。認証情報が正しい場合は、Windows アカウントおよび Credential Manager にログオンします。

アカウントの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Windows Logon]**（Windows のログオン）→**[Add a Network Account]**（ネットワーク アカウントの追加）の順にクリックします。[Add Network Account Wizard]（ネットワーク アカウントの追加ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

アカウントの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Windows Logon]**（Windows のログオン）→**[Manage Network Accounts]**（ネットワーク アカウントの管理）の順にクリックします。**[Manage Network Accounts]**ダイアログ ボックスが表示されます。
4. 削除するアカウントをクリックして**[Remove]**（削除）をクリックします。
5. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
6. **[OK]**をクリックします。

シングルサインオンの使用

Credential Manager には、複数のインターネットおよび Windows プログラム用のユーザ名とパスワードを格納し、ユーザが登録されたプログラムにアクセスすると自動的にログオン証明情報を入力する、シングルサインオン機能があります。

注記： シングルサインオンの重要な機能は、セキュリティとプライバシです。証明情報はすべて暗号化されており、Credential Manager へのログオンに成功した後にだけ使用できます。

注記： セキュリティ保護されたサイトまたはプログラムにログオンする前に、Java Card、指紋認証システム、またはトークンを使用して認証証明情報を検証するように、シングルサインオンを設定することもできます。この機能は、銀行口座番号などの個人情報が含まれているプログラムまたは Web サイトにログオンする場合に特に有効です。詳しくは、26 ページの「Credential Manager の設定」を参照してください。

新しいアプリケーションの登録

Credential Manager では、Credential Manager にログオンしている間に起動するアプリケーションをすべて登録するよう要求されます。アプリケーションを手動で登録することもできます。

自動登録の使用

1. ログオンが必要なアプリケーションを起動します。
2. プログラムまたは Web サイトのパスワード ダイアログ ボックスで[Credential Manager SSO]（証明情報マネージャ シングルサインオン）アイコンをクリックします。
3. プログラムまたは Web サイトのパスワードを入力して**[OK]**をクリックします。**[Credential Manager Single Sign On]**（証明情報マネージャ シングルサインオン）ダイアログ ボックスが開きます。

4. **[More]**（詳細）をクリックして以下のオプションのどれかを選択します。
   - [Do not use SSO for this site or application.]（このサイトまたはアプリケーションではシングルサインオン（SSO）を使用しない。）
   - [Prompt to select account for this application.]（このアプリケーションのアカウントの選択画面を表示する。）
   - [Fill in credentials but do not submit.]（証明情報を入力するが送信はしない。）
   - [Authenticate user before submitting credentials.]（証明情報を送信する前にユーザ認証を行う。）
   - [Show SSO shortcut for this application.]（このアプリケーションの SSO ショートカットを表示する。）
5. **[Yes]**（はい）をクリックして、登録を完了します。

手動（ドラッグ アンド ドロップ）登録の使用

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルで、**[Single Sign On]**（シングルサインオン）→**[Register New Application]**（新しいアプリケーションの追加）の順にクリックします。[SSO Application Wizard]（SSO アプリケーション ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

アプリケーションおよび証明情報の管理

アプリケーション プロパティの変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。
4. 変更するアプリケーション エントリをクリックして**[Properties]**.（プロパティ）をクリックします。
5. **[General]**（全般）タブをクリックして、アプリケーション名および説明を変更します。該当する設定の横にあるチェック ボックスにチェックを入れるか外して、設定を変更します。
6. **[Script]**（スクリプト）タブをクリックして、SSO アプリケーション スクリプトを表示し、編集します。
7. **[OK]**をクリックします。

シングルサインオンからのアプリケーションの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。

3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。
4. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。
5. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
6. **[OK]**をクリックします。

アプリケーションのエクスポート

アプリケーションをエクスポートして、シングルサインオン アプリケーション スクリプトのバックアップ コピーを作成できます。このファイルは、後でシングルサインオン データの復元に使用できます。これは、証明情報だけが含まれている ID バックアップ ファイルを補うものとして機能します。

アプリケーションをエクスポートするには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。
4. エクスポートするアプリケーション エントリをクリックします。次に、**[More]**（詳細）→**[Applications]**（アプリケーション）→**[Export Script]**（スクリプトのエクスポート）の順にクリックします。
5. 画面の説明に沿って操作し、エクスポートを完了します。
6. **[OK]**をクリックします。

アプリケーションのインポート

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。
4. インポートするアプリケーション エントリをクリックします。次に、**[More]**（詳細）→**[Applications]**（アプリケーション）→**[Import Script]**（スクリプトのインポート）の順に選択します。
5. 画面の説明に沿って操作し、インポートを完了します。
6. **[OK]**をクリックします。

証明情報の変更

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Single Sign On]**（シングルサインオン）で、**[Manage Applications and Credentials]**（アプリケーションおよび証明情報の管理）をクリックします。

4. 変更するアプリケーション エントリをクリックして**[More]**（詳細）をクリックします。
5. 以下のオプションのどれかを選択します。
   - Applications（アプリケーション）
     - Add New（新規追加）
     - Remove（削除）
     - Properties（プロパティ）
     - Import Script（スクリプトのインポート）
     - Export Script（スクリプトのエクスポート）
   - 証明情報
     - Create New（新規作成）
   - View Password（パスワードの表示）

   注記： パスワードを表示するには、事前に ID の認証を行う必要があります。
6. 画面に表示される説明に沿って操作します。
7. **[OK]**をクリックします。

アプリケーションの保護機能の使用

この機能を使用して、アプリケーションへのアクセス設定を行えます。以下の基準に基づいてアクセスを制限できます。

- ユーザのカテゴリ
- 使用する時間
- 無操作の状態

アプリケーションへのアクセス制限

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。**[Application Protection Service]**（アプリケーション保護サービス）ダイアログ ボックスが表示されます。
4. アクセスを管理したいユーザのカテゴリを選択します。

   注記： カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）を選択する必要がある場合があります。
5. **[Add]**（追加）をクリックします。[Add a Program Wizard]（プログラムの追加ウィザード）が起動します。
6. 画面に表示される説明に沿って操作します。

アプリケーションの保護の解除

アプリケーションのアクセス制限を解除するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。**[Application Protection Service]**（アプリケーション保護サービス）ダイアログ ボックスが表示されます。
4. アクセスを管理したいユーザのカテゴリを選択します。

   注記：　カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要がある場合があります。

5. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。
6. **[OK]**をクリックします。

保護されたアプリケーションの制限設定の変更

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
3. 右側のパネルの**[Application Protection]**（アプリケーションの保護）で、**[Manage Protected Applications]**（保護されたアプリケーションの管理）をクリックします。**[Application Protection Service]**（アプリケーション保護サービス）ダイアログ ボックスが表示されます。
4. アクセスを管理したいユーザのカテゴリを選択します。

   注記：　カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要がある場合があります。

5. 変更するアプリケーションをクリックして**[Properties]**（プロパティ）をクリックします。そのアプリケーションの**[Properties]**（プロパティ）ダイアログ ボックスが開きます。
6. **[General]**（全般）タブをクリックします。以下の設定のどれかを選択します。
   - [Disabled (Cannot be used)]（無効（使用不可））
   - [Enabled (Can be used without restrictions)]（有効（無制限に使用可能））
   - [Restricted (Usage depends on settings)]（制限あり（使用制限は設定により異なる））
7. [Restricted]（制限あり）を選択した場合、以下の設定が利用可能になります。

   a. 時間、曜日、または日付に基づいて使用を制限する場合は、**[Schedule]**（スケジュール）タブをクリックして設定を行います。

   b. 無操作状態に基づいて使用を制限する場合は、**[Advanced]**（詳細）タブをクリックして無操作の期間を選択します。

8. **[OK]**をクリックして、アプリケーションの**[Properties]**（プロパティ）ダイアログ ボックスを閉じます。

9. **[OK]**をクリックします。

高度なタスク（管理者のみ）

Credential Manager の[Authentication and Credentials]（認証および証明情報）ページおよび[Advanced Settings]（詳細設定）ページは、管理者権限を持つユーザだけが使用できます。これらのページから、次のタスクを実行できます。

- ユーザおよび管理者のログオン方法の指定
- カスタム認証要件の設定
- 証明情報のプロパティの設定
- Credential Manager の設定

ユーザおよび管理者のログオン方法の指定

[Authentication and Credentials]（認証および証明情報）ページで、ユーザまたは管理者のどちらかに、どのような種類または組み合わせの証明情報が必要かを指定できます。

ユーザまたは管理者のログオン方法を指定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Authentication and Credentials]**（認証および証明情報）の順にクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 一覧から、認証方法の種類または組み合わせをクリックします。
6. **[Apply]**（適用）→**[OK]**の順にクリックします。

カスタム認証要件の設定

[Authentication and Credentials]（認証および証明情報）ページの[Authentication]（認証）タブに、必要な認証証明情報のセットが一覧表示されない場合は、カスタム要件を作成できます。

カスタム要件を設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Authentication and Credentials]**（認証および証明情報）の順にクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 認証方法の一覧から、**[Custom]**（カスタム）をクリックします。
6. **[Configure]**（設定）をクリックします。
7. 使用する認証方法を選択します。
8. 以下のどちらかの項目をクリックして、方法の組み合わせを選択します。
   - AND を使用して認証方法を組み合わせる

     （ユーザはログオンするたびに、チェックを入れたすべての方法で認証する必要があります）
   - OR を使用して複数の認証方法のうち 1 つを要求する

     （ユーザはログオンするたびに、チェックを入れた方法のどれかを選択できます）
9. **[OK]**をクリックします。
10. **[Apply]**（適用）→**[OK]**の順にクリックします。

証明情報のプロパティの設定

[Authentication and Credentials]（認証および証明情報）ページの[Credentials]（証明情報）タブで、使用可能な認証方法の一覧を表示して設定を変更できます。

証明情報を設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Authentication and Credentials]**（認証および証明情報）の順にクリックします。
3. 右側のパネルで、**[Credentials]**（証明情報）タブをクリックします。

4. 変更する証明情報の種類をクリックします。次のどれかの方法で証明情報を変更できます。
   - 証明情報を登録するには、**[Register]**（登録）をクリックし、画面の説明に沿って操作します。
   - 証明情報を削除するには、**[Clear]**（クリア）をクリックし、確認ダイアログ ボックスで **[Yes]**（はい）をクリックします。
   - 証明情報のプロパティを変更するには、**[Properties]**（プロパティ）をクリックし、画面の説明に沿って操作します。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

Credential Manager の設定

[Settings]（設定）ページから、以下のタブを使用して各種の設定にアクセスし、変更することができます。

- General（全般）：基本的な設定を変更できます。
- Single Sign On（シングルサインオン）：現在のユーザに対するシングルサインオンの動作方法の設定（たとえば、ログオン画面の検出、登録されたログオン ダイアログへの自動ログオン、パスワードの表示などの処理方法）を変更できます。
- Services and Applications（サービスおよびアプリケーション）：使用可能なサービスを表示して、それらのサービスの設定を変更できます。
- Security（セキュリティ）：指紋認証ソフトウェアを選択して、指紋認証システムのセキュリティ レベルを調整できます。
- Smart Cards and Tokens（スマート カードおよびトークン）：使用可能なすべての Java Card およびトークンのプロパティを表示して変更できます。

Credential Manager の設定を変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、変更する設定が含まれるタブをクリックします。
4. 画面の説明に沿って操作し、設定を変更します。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、**[General]**（全般）タブをクリックします。
4. **[Select the way users log on to Windows (requires restart)]**（ユーザが Windows へログオンする方法の選択（再起動が必要））で、**[Use Credential Manager with classic logon prompt]**（証明情報マネージャでクラシック ログオン画面を使用する）チェック ボックスにチェックを入れます。

5. **[Apply]**（適用）→**[OK]**の順にクリックします。

6. コンピュータを再起動します。

注記： **[Use Credential Manager with classic logon prompt]**（証明情報マネージャでクラシックログオン画面を使用する）チェック ボックスにチェックを入れると、コンピュータをロックできるようになります。17 ページの 「コンピュータのロック」を参照してください。

例 2：[Advanced Settings]（詳細設定）ページを使用して、シングルサインオンの前にユーザ確認を要求する方法

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Settings]**（設定）の順にクリックします。
3. 右側のパネルで、**[Single Sign On]**（シングルサインオン）タブをクリックします。
4. **[When registered logon dialog or Web page is visited]**（登録したログオン ダイアログまたは Web ページが表示された時の動作）で、**[Authenticate user before submitting credentials]**（証明情報を送信する前にユーザの認証を行う）チェック ボックスにチェックを入れます。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。
6. コンピュータを再起動します。

3 Embedded Security for HP ProtectTools

注記： Embedded Security for HP ProtectTools を使用するには、統合された TPM（Trusted Platform Module）セキュリティ チップがコンピュータに内蔵されている必要があります。

Embedded Security for HP ProtectTools は、ユーザ データや証明情報を不正なアクセスから保護します。このソフトウェア モジュールには、以下のセキュリティ機能があります。

- 高度な Microsoft® EFS（Encryption File System）ファイルおよびフォルダの暗号化
- ユーザ データを保護するための PSD（Personal Secure Drive）の作成
- データ管理機能（キー階層のバックアップや復元など）
- Embedded Security ソフトウェアの使用時にデジタル証明情報の操作を保護するための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）のサポート

TPM 内蔵セキュリティ チップを使用すると、HP ProtectTools セキュリティマネージャの他のセキュリティ機能を強化したり有効にしたりできます。たとえば、Credential Manager for HP ProtectTools では、内蔵チップを Windows へのログオン時の認証要素として使用できます。一部のモデルでは、TPM 内蔵セキュリティ チップを使用して、BIOS Configuration for HP ProtectTools からアクセスする高度な BIOS セキュリティ機能を有効にすることもできます。

セットアップ手順

△ **注意：** セキュリティ上の危険にさらされないようにするために、IT 管理者が内蔵セキュリティ チップを直ちに初期化することを強くおすすめします。内蔵セキュリティ チップを初期化しない場合、不正なユーザ、コンピュータ ワーム、またはウィルスがコンピュータのオーナシップを奪い、緊急リカバリ アーカイブの処理やユーザ アクセスの設定など所有者のタスクを制御してしまう可能性があります。

以下の 2 つの項目の手順に沿って操作し、内蔵セキュリティ チップを有効にして初期化します。

内蔵セキュリティ チップの有効化

内蔵セキュリティ チップは、[Computer Setup]ユーティリティで有効にする必要があります。この手順は、BIOS Configuration for HP ProtectTools では実行できません。

内蔵セキュリティ チップを有効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に F10 キーを押して、コンピュータ セットアップ（F10）ユーティリティを起動します。
2. 管理者パスワードを設定していない場合は、矢印キーを使用して**[Security]**（セキュリティ）→**[Setup password]**（セットアップ パスワード）の順に選択して、Enter キーを押します。
3. **[New password]**（新しいパスワード）ボックスと**[Verify Password]**（パスワードの確認）ボックスにパスワードを入力して確定します。
4. **[Security]**（セキュリティ設定）メニューで、矢印キーを使用して**[TPM Embedded Security]**（TPM 内蔵セキュリティ）を選択し、Enter キーを押します。
5. **[Embedded Security]**（内蔵セキュリティ）にデバイスが表示されない場合、**[Available]**（利用可能）を選択します。
6. **[Embedded security device state]**（内蔵セキュリティ デバイスの状態）を選択し、**[Enable]**（有効にする）に変更します。
7. F10 キーを押して、Embedded Security の設定への変更を確定します。
8. 設定を保存してコンピュータ セットアップ（F10）ユーティリティを終了するには、矢印キーを使用して**[File]**（ファイル）→**[Save Changes and Exit]**（変更を保存して終了）の順に選択します。次に、画面の説明に沿って操作します。

内蔵セキュリティ チップの初期化

内蔵セキュリティの初期化プロセスでは、以下のことを行います。

- 内蔵セキュリティ チップの所有者のパスワードを設定します。これにより、内蔵セキュリティ チップ上のすべての所有者機能へのアクセスが保護されます。
- 緊急リカバリ アーカイブをセットアップします。緊急リカバリ アーカイブとは、すべてのユーザの基本ユーザ キーを再暗号化できるようにするための保護された記憶領域です。

内蔵セキュリティ チップを初期化するには、以下の手順で操作します。

1. タスク バーの右端の通知領域にある[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンを右クリックして、**[Embedded Security Initialization]**（内蔵セキュリティの初期化）を選択します。

   [HP ProtectTools Embedded Security Initialization Wizard]（HP ProtectTools Embedded Security 初期化ウィザード）が起動します。

2. 画面に表示される説明に沿って操作します。

基本ユーザ アカウントのセットアップ

Embedded Security で基本ユーザ アカウントをセットアップすると、次のタスクが実行されます。

- 暗号化された情報を保護するための基本ユーザ キーが生成され、その基本ユーザ キーを保護するための基本ユーザ キーのパスワードが設定されます。
- 暗号化されたファイルおよびフォルダを格納するための PSD（Personal Secure Drive）が設定されます。

△ **注意：** 基本ユーザ キーのパスワードは保護しておいてください。このパスワードがないと、暗号化されたデータにアクセスしたり復元したりできなくなります。

基本ユーザ アカウントをセットアップしてユーザ セキュリティ機能を有効にするには、以下の手順で操作します。

1. Embedded Security User Initialization Wizard（Embedded Security ユーザ初期化ウィザード）が起動していない場合は、**[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザーの設定）の順にクリックします。
3. 右側のパネルで、**[Embedded Security Features]**（内蔵セキュリティの機能）の**[Configure]**（設定）をクリックします。

   [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

   注記： セキュリティ保護された電子メールを使用するには、最初に、Embedded Security で作成されたデジタル証明情報を使用するように電子メール クライアントを設定する必要があります。デジタル証明情報が使用できない場合は、証明機関から取得する必要があります。電子メールを設定してデジタル証明情報を取得する手順については、電子メール クライアントのヘルプを参照してください。

一般的なタスク

基本ユーザ アカウントのセットアップを完了すると、以下のタスクを実行できます。

- ファイルおよびフォルダの暗号化
- 暗号化された電子メールの送受信

Personal Secure Drive（PSD）の使用

PSD のセットアップを完了すると、次回のログオンで、基本ユーザ キーのパスワードを入力するよう要求されます。基本ユーザ キーのパスワードを正しく入力すると、Windows エクスプローラから直接 PSD にアクセスできます。

ファイルおよびフォルダの暗号化

暗号化ファイルを操作する場合は、以下の規則を考慮してください。

- 暗号化できるファイルおよびフォルダは、NTFS パーティション上のものだけです。FAT パーティション上のファイルおよびフォルダは暗号化できません。
- システム ファイルや圧縮されたファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時フォルダは、ハッカーの関心を引く可能性があるため、暗号化するようにしてください。
- ファイルまたはフォルダを初めて暗号化した時、回復ポリシーが自動的にセットアップされます。暗号化証明情報や秘密キーをなくした場合でも、このポリシーによって、回復エージェントを使用して情報の暗号化を解除できるようになります。

ファイルおよびフォルダを暗号化するには、以下の手順で操作します。

1. 暗号化するファイルまたはフォルダを右クリックします。
2. **[Encrypt]**（暗号化）をクリックします。
3. 以下のオプションのどちらかをクリックします。
   - **[Apply changes to this folder only]**（このフォルダにのみ変更を適用する）
   - **[Apply changes to this folder, subfolders, and files]**（このフォルダ、およびサブフォルダとファイルに変更を適用する）
4. **[OK]**をクリックします。

暗号化された電子メールの送受信

Embedded Security では、暗号化された電子メールの送受信を行うことができますが、その手順は電子メールのアクセスに使用しているプログラムによって異なります。詳しくは、Embedded Security のヘルプおよび使用している電子メール アプリケーションのヘルプを参照してください。

基本ユーザ キーのパスワードの変更

基本ユーザ キーのパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザーの設定）の順にクリックします。
3. 右側のパネルで、**[Basic User Key password]**（基本ユーザ キーのパスワード）の**[Change]**（変更）をクリックします。
4. 古いパスワードを入力した後、新しいパスワードを設定して確定します。
5. **[OK]**をクリックします。

高度なタスク

バックアップおよび復元

Embedded Security のバックアップ機能では、緊急の場合に復元される証明情報を含むアーカイブが作成されます。

バックアップ ファイルの作成

バックアップ ファイルを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Backup]**（バックアップ）をクリックします。Embedded Security Backup Wizard（Embedded Security バックアップ ウィザード）が開きます。
4. 画面に表示される説明に沿って操作します。

バックアップ ファイルからの証明データの復元

バックアップ ファイルからデータを復元するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Restore]**（復元）をクリックします。Embedded Security Backup Wizard（Embedded Security バックアップ ウィザード）が開きます。
4. 画面に表示される説明に沿って操作します。

所有者のパスワードの変更

所有者のパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Owner Password]**（所有者のパスワード）の**[Change]**（変更）をクリックします。
4. 古い所有者のパスワードを入力した後、新しい所有者のパスワードを設定して確定します。
5. **[OK]**をクリックします。

ユーザ パスワードの再設定

ユーザが忘れたパスワードを管理者に再設定してもらうことができます。詳しくは、ヘルプを参照してください。

Embedded Security の有効化および無効化

セキュリティ機能を使用しないで操作する場合は、Embedded Security の機能を無効にすることができます。

Embedded Security の機能は、次の 2 種類のレベルで有効または無効にすることができます。

- 一時的な無効化：このオプションを使用すると、Windows の再起動時に Embedded Security が自動的に再び有効になります。このオプションは、初期設定ですべてのユーザが使用できます。
- 永続的な無効化：このオプションを使用すると、Embedded Security を再び有効にするには所有者のパスワードが必要になります。このオプションは、管理者だけが使用できます。

Embedded Security の永続的な無効化

Embedded Security を永続的に無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Embedded Security]**の**[Disable]**（無効にする）をクリックします。
4. 入力画面で所有者のパスワードを入力して**[OK]**をクリックします。

Embedded Security の永続的な無効化の後の有効化

Embedded Security を永続的に無効にした後で再び有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Embedded Security]**の**[Enable]**（有効にする）をクリックします。
4. 入力画面で所有者のパスワードを入力して**[OK]**をクリックします。

移行ウィザードによるキーの移行

移行は、キーや証明情報の管理、復元、転送などを行うことができる、高度な管理者タスクです。

移行について詳しくは、Embedded Security のヘルプを参照してください。

4 Java Card Security for HP ProtectTools

Java Card Security for HP ProtectTools は、オプションのカード リーダーが装備されたコンピュータでの Java Card のセットアップおよび設定を管理します。

Java Card Security を使用すると、次のタスクを実行できます。

- Java Card のセキュリティ機能にアクセスできます。
- [Computer Setup]ユーティリティを使用して、電源投入時の環境で Java Card の認証を有効にすることができます。
- Java Card を管理者およびユーザに個別に設定できます。オペレーティング システムがロードされる前に、ユーザは Java Card を挿入し、PIN を入力する必要があります。
- Java Card のユーザ認証を行うための PIN の設定および変更を行えます。

一般的なタスク

[General]（全般）ページを使用すると、次のタスクを実行できます。

- Java Card の PIN の変更
- カード リーダーまたはスマート カード キーボードの選択

注記： カード リーダーでは、Java Card とスマート カードの両方を使用します。この機能は、コンピュータに複数のカード リーダーが装備されている場合に使用できます。

Java Card の PIN の変更

Java Card の PIN を変更するには、以下の手順で操作します。

注記： Java Card の PIN は、4 ～ 8 桁の半角数字にする必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. PIN が設定されている Java Card をカード リーダーに挿入します。
4. 右側のパネルで、**[Change]**（変更）をクリックします。
5. **[Change PIN]**（PIN の変更）ダイアログ ボックスで、**[Current PIN]**（現在の PIN）ボックスに現在の PIN を入力します。
6. **[New PIN]**（新しい PIN）ボックスに新しい PIN を入力し、**[Confirm New PIN]**（新しい PIN の確認入力）ボックスに PIN を再度入力します。
7. **[OK]**をクリックします。

カード リーダーの選択

Java Card を使用する前に、Java Card Security for ProtectTools で正しいカード リーダーが選択されていることを確認してください。正しいリーダーが選択されていないと、一部の機能が使用できなくなるか、正しく表示されない場合があります。さらに、カード リーダー ドライバが正しくインストールされ、Windows の[デバイス マネージャ]に正しく表示される必要があります。

カード リーダーを選択するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[General]**（全般）をクリックします。
3. Java Card をカード リーダーに挿入します。
4. 右側のパネルの**[Selected card reader]**（スマート カード リーダー）で正しいリーダーをクリックします。

高度なタスク（管理者のみ）

[Advanced]（アドバンス）ページを使用すると、次のタスクを実行できます。

- Java Card の PIN の割り当て
- Java Card への名前の割り当て
- 電源投入時認証の設定
- Java Card のバックアップおよびリストア（復元）

注記： **[Advanced]**（アドバンス）ページを表示するには、Windows 管理者権限を持っている必要があります。

Java Card の PIN の割り当て

Java Card Security for ProtectTools で Java Card を使用できるようにするには、Java Card に名前と PIN を割り当てる必要があります。

Java Card に PIN を割り当てるには、以下の手順で操作します。

注記： Java Card の PIN は、4 ～ 8 桁の半角数字にする必要があります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. 新しい Java Card をカード リーダーに挿入します。
4. **[New Card]**（新しいカード）ダイアログ ボックスが表示されたら、**[New display name]**（新しい表示名）ボックスに新しい名前を、**[New PIN]**（新しい PIN）ボックスに新しい PIN を入力し、**[Confirm New PIN]**（新しい PIN の確認入力）ボックスに PIN を再度入力します。
5. **[OK]**をクリックします。

Java Card への名前の割り当て

電源投入時認証に Java Card を使用できるようにするには、Java Card に名前を割り当てる必要があります。

Java Card に名前を割り当てるには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. Java Card をカード リーダーに挿入します。

注記： このカードにまだ PIN を割り当てていない場合は、**[New Card]**（新しいカード）ダイアログ ボックスが表示され、ここで新しい名前および PIN を入力できます。

4. 右側のパネルで、**[Display name]**（表示名）の**[Change]**（変更）をクリックします。
5. **[Name]**（名前）ボックスに、Java Card の名前を入力します。
6. **[PIN]**ボックスに、現在の Java Card の PIN を入力します。
7. **[OK]**をクリックします。

電源投入時認証の設定

電源投入時認証が有効になると、Java Card を使用してコンピュータを起動することが必要になります。

Java Card の電源投入時認証を有効にするプロセスには、以下の手順が含まれます。

1. BIOS Configuration または[Computer Setup]ユーティリティで、Java Card の電源投入時認証サポートを有効にします。詳しくは、48 ページの 「スマート カードの電源投入時認証サポートの有効/無効の設定」を参照してください。
2. Java Card Security for ProtectTools で、Java Card の電源投入時認証を有効にします。
3. 管理者 Java Card を作成し、有効にします。

Java Card の電源投入時認証の有効化および管理者 Java Card の作成

Java Card の電源投入時認証を有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. Java Card をカード リーダーに挿入します。

   注記： このカードにまだ名前および PIN を割り当てていない場合は、**[New Card]**（新しいカード）ダイアログ ボックスが表示され、ここで新しい名前および PIN を入力できます。

4. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[Enable]**（有効にする）チェック ボックスにチェックを入れます。
5. **[Computer Setup Password]**（[Computer Setup]のパスワード）ダイアログ ボックスで、[Computer Setup]ユーティリティのパスワードを入力して**[OK]**をクリックします。
6. DriveLock をまだ有効にしていない場合は、Java Card の PIN を入力して**[OK]**をクリックします。

   または

   DriveLock をすでに有効にしている場合は、以下の手順で操作します。

   a. **[Make Java card identity unique]**（Java Card の ID を固有のものにする）をクリックします。

      または

      [Make the Java card identity the same as the DriveLock password]（Java Card の ID を DriveLock パスワードと同じにする）をクリックします。

      注記： コンピュータで DriveLock が有効になっていると、Java Card の ID を DriveLock の user password（ユーザ パスワード）と同じものに設定できます。これにより、コンピュータを起動するときに、Java Card のみを使用して DriveLock と Java Card の両方を認証できるようになります。

   b. 必要に応じて、**[DriveLock password]**（DriveLock パスワード）ボックスに DriveLock の user password（ユーザ パスワード）を入力し、**[Confirm password]**（パスワードの確認）ボックスにパスワードを再度入力します。

   c. Java Card の PIN を入力します。

   d. **[OK]**をクリックします。

7. リカバリ ファイルを作成するよう要求されたら、**[Cancel]**（キャンセル）をクリックして後でリカバリ ファイルを作成するか、または**[OK]**をクリックし、[HP ProtectTools Backup Wizard]（HP ProtectTools バックアップ ウィザード）の画面の説明に沿って操作し、ここでリカバリ ファイルを作成します。

   注記： 詳しくは、8 ページの 「HP ProtectTools Backup and Restore」を参照してください。

ユーザ Java Card の作成

注記： ユーザ Java Card を作成するには、電源投入時認証および管理者カードが設定されている必要があります。

ユーザ Java Card を作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. ユーザ カードとして使用する Java Card を挿入します。
4. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[User card identity]**（ユーザ用カードの ID）の横にある**[Create]**（作成）をクリックします。
5. ユーザ Java Card の PIN を入力して**[OK]**をクリックします。

Java Card の電源投入時認証の無効化

Java Card の電源投入時認証を無効にすると、コンピュータにアクセスするために Java Card を使用する必要はなくなります。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Java Card Security]**（Java Card セキュリティ）をクリックし、**[Advanced]**（アドバンス）をクリックします。
3. 管理者 Java Card を挿入します。
4. 右側のパネルで、**[Power-on authentication]**（電源投入時認証）の**[Enable]**（有効にする）チェック ボックスのチェックを外します。
5. Java Card の PIN を入力して**[OK]**をクリックします。

5 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools を使用すると、[Computer Setup]ユーティリティのセキュリティ設定にアクセスできます。これにより、[Computer Setup]で管理されるシステムのセキュリティ機能に Windows から簡単にアクセスできるようになります。

BIOS Configuration を使用すると、次のことを行えます。

- 電源投入時パスワードおよび管理者パスワードを管理できます。
- 内蔵セキュリティ認証サポートの有効化など、電源投入時のその他の認証機能を設定できます。
- CD-ROM のブートや各種ハードウェア ポートなど、ハードウェア機能を有効および無効に設定できます。
- マルチブートの有効化および起動順序の変更を含む、ブート オプションを設定できます。

注記： BIOS Configuration for HP ProtectTools にある機能の多くは、[Computer Setup]でも使用できます。

一般的なタスク

BIOS Configuration を使用すると、通常は起動時に F10 キーを押してコンピュータ セットアップ（F10）ユーティリティを使用することでしかアクセスできない、各種のコンピュータ設定を管理できます。

ブート オプションの管理

BIOS Configuration を使用すると、コンピュータの起動や再起動に実行されるタスクに対する各種の設定を管理できます。

ブート オプションを管理するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。

   注記： BIOS の管理者パスワードの入力画面は、[Computer Setup]のパスワードがすでに設定されている場合にのみ表示されます。[Computer Setup]のパスワードの設定について詳しくは、52 ページの「セットアップ パスワードの設定」を参照してください。

4. 左側のパネルで、**[System Configuration]**（システム コンフィギュレーション）をクリックします。
5. 右側のパネルで、F9、F10、および F12 と、**[Express Boot Popup Delay（Sec）]**（高速ブートポップアップ遅延（秒））に対する遅延時間（秒単位）を選択します。
6. **[MultiBoot]**（マルチブート）を有効または無効にします。
7. マルチブートを有効にしている場合は、ブート デバイスを選択し、上向きの矢印または下向きの矢印をクリックして一覧内の順序を調整することで、起動順序を選択します。
8. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

システム コンフィギュレーション オプションの有効/無効の設定

注記：　次の項目の一部は、お使いのコンピュータでサポートされていない場合があります。

デバイスまたはセキュリティ オプションの有効/無効を切り替えるには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。
4. 左側のパネルで**[System Configuration]**（システム コンフィギュレーション）をクリックしてから、システム コンフィギュレーション オプションの有効/無効を切り替えるか、右側のパネルで次のどれかのシステム コンフィギュレーション オプションの設定を行います。
   - Port Options（ポート オプション）
     - Serial Port（シリアル ポート）
     - Infrared Port（赤外線ポート）
     - Parallel Port（パラレル ポート）
     - SD Slot（SD スロット）
     - USB Port（USB ポート）
     - 1394 Port（1394 ポート）
     - Cardbus Slot（CardBus スロット）
     - ExpressCard slot（ExpressCard スロット）
   - Boot Options（ブート オプション）
     - F9, F10, and F12 Delay (Sec)（F9、F10、および F12 の遅延（秒））
     - MultiBoot（マルチブート）
     - Express Boot Popup Delay (Sec)（高速ブート ポップアップ遅延（秒））
     - CD-ROM Boot（CD-ROM ドライブからのブート）
     - Floppy Boot（ディスケット ドライブからのブート）
     - Internal Network Adapter Boot（内蔵ネットワーク アダプタ ブート）
     - Internal Network Adapter Boot Mode (PXE or RPL)（内蔵ネットワーク アダプタ ブート モード（PXE または RPL））
     - Boot Order（ブート順序）
   - Device Configurations（デバイス設定）
     - NumLock at Boot（ブート時 NumLock）
     - Swapping fn/ctrl Keys（[fn]/[ctrl]キーの切り替え）
     - Multiple Pointing Devices（マルチポインティング デバイス）
     - USB Legacy Support（USB レガシー サポート）

- Parallel port mode (standard, bidirectional, EPP, or ECP)（パラレル ポート モード：EPP（Enhanced Parallel Port）、標準、双方向、または ECP（Enhanced Capabilities Port））
- Data Execution Prevention（データ実行防止）
- SATA Native Mode（SATA ネイティブ モード）
- Dual Core CPU（デュアル コア CPU）
- Automatic Intel® SpeedStep Functionality Support（Automatic Intel SpeedStep 機能サポート）
- Fan Always on While on AC Power（外部電源の使用中は常にファンをオンにする）
- BIOS DMA Data Transfers（BIOS ATA DMA 転送）
- Intel or AMD PSAE Execution Disable（Intel または AMD PSAE の実行無効設定）

● Built-In Device Options（内蔵デバイス オプション）
  - Embedded WLAN Device Radio（内蔵無線 LAN デバイスの無線）
  - Embedded WWAN Device Radio（内蔵無線 WAN デバイスの無線）
  - Embedded Bluetooth® Device Radio（内蔵 Bluetooth デバイスの無線）
  - LAN/WLAN Switching（LAN/無線 LAN の切り替え）
  - Wake on LAN from Off（電源オフ状態からの Wake on LAN の実行）

5. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックして変更を保存してから終了します。

高度なタスク

HP ProtectTools アドオン モジュールの設定の管理

HP ProtectTools セキュリティ マネージャの一部の機能は、BIOS Configuration で管理できます。

スマート カードの電源投入時認証サポートの有効/無効の設定

このオプションを有効にすると、コンピュータの電源投入時のユーザ認証にスマート カードを使用できます。

注記： 電源投入時認証機能を完全に有効にするには、Java Card Security for HP ProtectTools モジュールを使用してスマート カードも設定する必要があります。

スマート カードの電源投入時認証サポートを有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]** をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Smart Card Security]**（スマート カード セキュリティ）で、**[Enable]**（有効にする）をクリックします。

   注記： スマート カード電源投入時認証を無効にするには、**[Disable]**（無効にする）をクリックします。
6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

内蔵セキュリティの電源投入時認証サポートの有効/無効の設定

このオプションを有効にすると、TPM 内蔵セキュリティ チップ（使用可能な場合のみ）をコンピュータの電源投入時のユーザ認証に使用できます。

注記：　電源投入時認証機能を完全に有効にするには、Embedded Security for HP ProtectTools モジュールを使用して TPM 内蔵セキュリティ チップも設定する必要があります。

内蔵セキュリティの電源投入時認証サポートを有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）をクリックします。
3. BIOS の管理者パスワードの入力画面で[Computer Setup]の管理者パスワードを入力して、**[OK]**をクリックします。
4. 左側のパネルで、**[Security]**（セキュリティ）をクリックします。
5. **[Embedded Security]**（内蔵セキュリティ）で、**[Power-on Authentication Support]**（電源投入時認証サポート）の隣の**[Enable]**（有効にする）をクリックします。

   注記：　内蔵セキュリティの電源投入時認証を無効にするには、**[Disable]**（無効にする）をクリックします。
6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

DriveLock によるハードディスク ドライブ保護の有効/無効の設定

ドライブロックは、ATA ハードディスク ドライブにあるデータへの不正アクセスを防止する業界標準のセキュリティ機能です。コンピュータ セットアップ（F10）ユーティリティの拡張機能として実装されています。この機能は、ATA Security コマンド セットに対応するハードディスク ドライブが検出された場合にのみ利用できます。ドライブロックは、データのセキュリティを最重要視するユーザ向けに開発されました。このようなユーザにとっては、ハードディスク ドライブのコストとそこに格納されているデータの喪失は、データへの不正アクセスの結果生じる可能性のある損害に比べれば、些細なものです。このレベルのセキュリティの確保と同時に、パスワードを忘れたときの対処もできるように、HP が実装したドライブロックでは、2 つのパスワードによるセキュリティ方式を採用しています。一方のパスワードはシステム管理者が設定して使用するもので、もう一方のパスワードは通常、エンド ユーザが設定して使用します。両方のパスワードを忘れてしまった場合にドライブをアンロックするための手段はありません。したがって、ハードディスク ドライブに含まれるデータが企業情報システムに複製されているか、または定期的にバックアップが作成されている場合に、ドライブロックを最も安全に使用できます。ドライブロックの両方のパスワードを忘れてしまった場合は、ハードディスク ドライブを使用できなくなります。前に述べたカスタマ プロファイルに適合しないすべてのユーザにとって、この事実は受け入れ難いリスクになる可能性があります。一方、カスタマ プロファイルに適合するユーザにとっては、ハードディスク ドライブに保存されたデータの性質上、許容できるリスクだと言えます。

ドライブロックの使用法

ATA Security コマンド セットに対応するハードディスク ドライブが 1 つ以上検出された場合、**[ドライブロック]**（DriveLock）オプションは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）メニューに表示されます。ユーザには、マスタ パスワード（master password）を設定したりドライブロックを有効にしたりするオプションが提供されます。ドライブロックを有効にするには、ユーザ パスワード（user password）を入力する必要があります。通常、ドライブロックの最初のコンフィギュレーションはシステム管理者が実行するため、マスタ パスワードを最初に設定する必要があります。ドライブロックを有効にするか無効のままにしておくかにかかわらず、管理者はマスタ パスワードを設定することをおすすめします。これにより、将来ドライブがロックされた場合に、管理者はドライブロックの設定値を変更できるようになります。マスタ パスワードが設定されると、システム管理者はいつでもドライブロックの有効/無効を切り替えることができます。

ロックされたハードディスク ドライブが存在する場合は、POST（Power-On Self Test）によって、そのドライブをアンロックするためのパスワードが要求されます。電源投入時パスワード（power-on password）が設定されていて、そのドライブのユーザ パスワードと一致する場合は、パスワードの再入力は要求されません。一致しない場合は、ドライブロックのパスワードを入力するよう要求されます。コールド ブート時には、マスタ パスワードとユーザ パスワードのどちらも使うことができます。ウォーム ブート時には、コールド ブートの前にドライブのロック解除に使用したパスワードと同じものを入力します。ユーザは、パスワードが正しいと認識されるまで、2 回入力できます。コールド ブート時には、2 回とも間違えた場合でも POST は続行されますが、そのドライブにはアクセスできません。ウォーム ブート時または Windows からの再起動時には、2 回とも間違えた場合は POST が停止され、再起動するよう求められます。

ドライブロックの使用例

ドライブロックのセキュリティ機能は、企業環境での使用に最も適しています。システム管理者はハードディスク ドライブのコンフィギュレーションを担当しますが、その作業には、ドライブロックのマスタ パスワードおよび一時ユーザ パスワードを設定することが含まれます。ユーザがユーザ パスワードを忘れた場合や、コンピュータを別の従業員が使うことになった場合、システム管理者はマスタ パスワードを使用して、ユーザ パスワードをリセットしたり、ハードディスク ドライブへのアクセス権を回復したりすることができます。

企業システム管理者は、ドライブロックを有効にする場合、マスタ パスワードの設定とメンテナンスについての企業方針を確立しておくことをおすすめします。これは、従業員が会社を辞める前に意図的に、または誤ってドライブロックの両方のパスワードを設定してしまうという状況を防ぐために必要です。両方のパスワードを設定した従業員が会社を辞めてしまった場合、そのハードディスク ドライブは使用不能となり、交換が必要になります。また、マスタ パスワードが設定されていないと、シ

ステム管理者がロックされたハードディスク ドライブにアクセスできなくなり、不正ソフトウェアの日常チェックや、その他の資産管理およびサポートを実行できなくなることがあります。

それほど厳重なセキュリティを必要としないユーザの場合は、ドライブロックを有効にしないことをおすすめします。この種のユーザには、個人ユーザや、機密性の高いデータをハードディスク ドライブに保持しないことを習慣にしているユーザが含まれます。このようなユーザにとっては、両方のパスワードを忘れてハードディスク ドライブが使えなくなることのほうが、ドライブロックにより保護されるデータの価値よりもはるかに大きな問題と言えます。コンピュータ セットアップ（F10）ユーティリティとドライブロックへのアクセスは、セットアップ パスワードによって制限できます。セットアップ パスワードを指定してそれをエンド ユーザに公表しないことで、システム管理者はユーザがドライブロックを有効にできないようにします。

[Computer Setup]のパスワードの管理

BIOS Configuration を使用すると、[Computer Setup]の電源投入時パスワードやセットアップ パスワードの設定および変更を行うことができるほか、各種のパスワード設定も管理できます。

△ **注意：** BIOS Configuration の[Passwords]（パスワード）ページで設定したパスワードは、[HP ProtectTools]ウィンドウの**[Apply]**（適用）または**[OK]**ボタンをクリックすると直ちに保存されます。パスワード設定を元に戻す場合も以前のパスワードを指定する必要があるため、設定したパスワードを忘れないようにしてください。

電源投入時パスワードは、ノートブック コンピュータを不正な使用から保護できます。

注記： 電源投入時パスワードを設定すると、[Passwords]ページの[Set]（設定）ボタンが[Change]（変更）ボタンに置き換えられます。

[Computer Setup]のパスワードは、[Computer Setup]内の設定値とシステム識別情報を保護します。いったんこのパスワードを設定すると、次回から[Computer Setup]へのアクセスにはこのパスワードの使用が必要になります。セットアップ パスワードを設定している場合は、HP ProtectTools の BIOS Configuration の部分を起動する前にパスワードを入力するよう要求されます。

注記： セットアップ パスワードを設定すると、[Passwords]ページの[Set]ボタンが[Change]ボタンに置き換えられます。

電源投入時パスワードの設定

電源投入時パスワードを設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Power-On Password]**（電源投入時パスワード）の隣の**[Set]**（設定）をクリックします。
4. **[Enter Password]**（パスワードの入力）および**[Verify Password]**（パスワードの確認）ボックスにパスワードを入力して確定します。
5. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

電源投入時パスワードの変更

電源投入時パスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Power-On Password]**（電源投入時パスワード）の隣の**[Change]**（変更）をクリックします。
4. **[Old Password]**（古いパスワード）ボックスに、現在のパスワードを入力します。
5. **[Enter New Password]**（新しいパスワードの入力）ボックスに新しいパスワードを設定して確定します。
6. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
7. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

セットアップ パスワードの設定

[Computer Setup]のパスワードを設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Setup Password]**（セットアップ パスワード）の隣の**[Set]**（設定）を選択します。
4. **[Enter Password]**（パスワードの入力）および**[Confirm Password]**（パスワードの確認）ボックスにパスワードを設定して確定します。
5. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
6. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

セットアップ パスワードの変更

[Computer Setup]のパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルで、**[Setup Password]**（セットアップ パスワード）の隣の**[Change]**（変更）をクリックします。
4. **[Old Password]**（古いパスワード）ボックスに、現在のパスワードを入力します。
5. **[Enter New Password]**（新しいパスワードの入力）および**[Verify new password]**（新しいパスワードの確認）ボックスに新しいパスワードを入力して確定します。
6. **[Passwords]**（パスワード）ダイアログ ボックスで**[OK]**をクリックします。
7. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

パスワード オプションの設定

BIOS Configuration for HP ProtectTools を使用すると、システムのセキュリティを強化するようにパスワード オプションを設定できます。

厳重なセキュリティの有効化および無効化

△ **注意：** コンピュータが永久に使用できなくなることを防ぐため、設定したセットアップ パスワード、電源投入時パスワード、またはスマート カードの PIN を、紙などに書いて他人の目にふれない安全な場所に保管しておいてください。これらのパスワードや PIN を忘れてしまうと、コンピュータのロックを解除できなくなります。

厳重なセキュリティを有効にすると、電源投入時パスワード、管理者パスワード、およびその他の電源投入時認証形式による保護が強化されます。

厳重なセキュリティを有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルの**[Password options]**（パスワード オプション）で、**[Stringent Security]**（厳重なセキュリティ）を有効または無効にします。

   注記： 厳重なセキュリティを無効にする場合は、**[Enable Stringent Security]**（厳重なセキュリティの有効化）チェック ボックスのチェックを外します。

4. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

Windows 再起動時の電源投入時認証の有効/無効の設定

このオプションを使用すると、Windows の再起動時にユーザに電源投入時、TPM、またはスマートカードの各パスワードの入力を要求することでセキュリティを強化できます。

Windows の再起動時の電源投入時認証を有効または無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**（BIOS 設定）→**[Security]**（セキュリティ）の順にクリックします。
3. 右側のパネルの**[Password options]**（パスワード オプション）で、**[Require password on restart]**（再起動時のパスワードの要求）を有効または無効にします。
4. [HP ProtectTools]ウィンドウで**[Apply]**（適用）→**[OK]**の順にクリックします。

6 Drive Encryption for HP ProtectTools

△ **注意：** Drive Encryption モジュールをアンインストールする場合は、まず、暗号化されたすべてのドライブの暗号化を解除する必要があります。そうしないと、Drive Encryption 復元サービスに登録していない限り、暗号化されたドライブ上のデータにアクセスできなくなります（58 ページの「復元」を参照してください）。Drive Encryption モジュールを再インストールしても、暗号化されたドライブにはアクセスできません。

暗号化の管理

ドライブの暗号化

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Encryption Management]**（暗号化の管理）の順にクリックします。
3. 右側のパネルで、**[Activate]**（有効にする）をクリックします。[Drive Encryption for HP ProtectTools Wizard]（Drive Encryption for HP ProtectTools ウィザード）が起動します。
4. 画面の説明に沿って操作し、暗号化を有効にします。

注記：　リカバリ情報を保存するためのディスケット、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアを指定する必要があります。

暗号化の変更

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Encryption Management]**（暗号化の管理）の順にクリックします。
3. 右側のパネルで、**[Change encryption]**（暗号化の変更）をクリックします。**[Change Encryption]**（暗号化の変更）ダイアログ ボックスで、暗号化するディスクを選択して**[OK]**をクリックします。
4. **[OK]**を再度クリックして、暗号化を開始します。

デバイスの暗号化解除

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Encryption Management]**（暗号化の管理）の順にクリックします。
3. 右側のパネルで、**[Deactivate]**（無効にする）をクリックします。

ユーザ管理

ユーザの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[Add]**（追加）をクリックします。**[User Name]**（ユーザ名）リストのユーザ名をクリックするか、または**[Username]**（ユーザ名）ボックスにユーザ名を入力します。**[Next]**（次へ）をクリックします。
4. 選択したユーザの Windows パスワードを入力して**[Next]**（次へ）をクリックします。
5. 新しいユーザの認証方法を選択して**[Finish]**（完了）をクリックします。

ユーザの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[User Name]**（ユーザ名）リストから削除するユーザ名をクリックします。**[Remove]**（削除）をクリックします。
4. **[Yes]**（はい）をクリックして、選択したユーザの削除を確定します。

トークンの変更

ユーザの認証方法を変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[User Name]**（ユーザ名）リストからユーザ名を選択して**[Change Token]**（トークンの変更）をクリックします。
4. ユーザの Windows パスワードを入力して**[Next]**（次へ）をクリックします。
5. 新しい認証方法を選択して**[Finish]**（完了）をクリックします。
6. 認証方法として Java Card を選択した場合は、入力を要求されたら Java Card のパスワードを入力して**[OK]**をクリックします。

パスワードの設定

パスワードの設定、またはユーザの認証方法の変更を行うには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[User Management]**（ユーザ管理）の順にクリックします。
3. 右側のパネルで、**[User Name]**（ユーザ名）リストからユーザを選択して**[Set Password]**（パスワードの設定）をクリックします。

4. ユーザの Windows パスワードを入力して**[Next]**（次へ）をクリックします。
5. 新しい認証方法を選択して**[Finish]**（完了）をクリックします。
6. 認証方法として Java Card を選択した場合は、入力を要求されたら Java Card のパスワードを入力して**[OK]**をクリックします。

復元

使用可能な安全策として、次の 2 つがあります。

- パスワードを忘れた場合は、暗号化されたドライブにアクセスできません。ただし、Drive Encryption 復元サービスに登録しておくと、パスワードを忘れた場合でもコンピュータにアクセスできるようになります。
- Drive Encryption キーを、ディスケット、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアにバックアップできます。

Drive Encryption 復元サービスへの登録

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Recovery]**（リカバリ）の順にクリックします。
3. 右側のパネルで、**[Click here to register]**（登録するにはここをクリック）をクリックします。要求された情報を入力して、セキュリティ バックアップ手順を完了します。

Drive Encryption キーのバックアップ

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[Drive Encryption]**（ドライブの暗号化）→**[Recovery]**（リカバリ）の順にクリックします。
3. 右側のパネルで、**[Click here to backup your keys]**（キーをバックアップするにはここをクリック）をクリックします。
4. リカバリ情報を保存するディスケット、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアを選択して**[Next]**（次へ）をクリックします。[Drive Encryption for HP ProtectTools Wizard]（Drive Encryption for HP ProtectTools ウィザード）が起動します。
5. 画面の説明に沿って操作し、Drive Encryption キーをバックアップします。

注記：　リカバリ情報を保存するためのディスケット、フラッシュ ストレージ デバイス、またはその他の USB 接続ストレージ メディアを指定する必要があります。

7 トラブルシューティング

Credential Manager for ProtectTools

簡単な説明	詳しい説明	解決方法
Credential Manager の [Network Accounts]（ネットワーク アカウント）オプションを使用すると、ログインするドメイン アカウントを選択できる。TPM 認証を使用する場合、このオプションは使用できない。他の認証方式はすべて正常に機能する	TPM 認証を使用する場合、ユーザはローカル コンピューにのみログインできます	Credential Manager のシングルサインオン ツールを使用すると、他のアカウントも認証できます
Windows XP SP1 へのログインで、USB トークンの証明書を使用できない	USB トークン ソフトウェアをインストールし、USB トークンの証明書を登録し、Credential Manager をプライマリ ログインとして設定しても、USB トークンは一覧に表示されません。また、Credential Manager/gina ログオンで使用することもできません Windows に再度ログインして、Credential Manager からログオフし、もう一度 Credential Manager にログインして、トークンをプライマリ ログインとして再選択すると、トークン ログイン操作が正常に機能します	この現象は、Windows XP Service Pack 1 でのみ発生します。Windows Update を使用して、Windows XP のバージョンを Service Pack 2 に更新すると問題は解決されます Service Pack 1 のままでこの問題を回避するには、別の証明書（Windows パスワード）を使用して Windows に再度ログインしてから、Credential Manager からログオフし、もう一度 Credential Manager にログインします
一部のアプリケーションの Web ページにエラーが表示され、タスクの実行や完了が不可能になる	シングルサインオンの機能パターンが無効になったことが原因で、一部の Web ベース アプリケーションが機能しなくなりエラーを報告します。たとえば、Internet Explorer では、黄色の三角形の中に**[!]**のマークが表示され、エラーの発生を通知します	Credential Manager シングルサインオンは、すべてのソフトウェア Web インタフェースをサポートするわけではありません。特定の Web ページでは、シングルサインオン サポートをオフにして、シングルサインオン サポートを無効にしてください。Credential Manager のヘルプ ファイルに用意されている、シングルサインオンについての詳しいドキュメントを参照してください 特定のアプリケーションでシングルサインオンを無効にできない場合は、HP のサポート窓口にお問い合わせください
ログイン プロセスで、**[Browse for Virtual Token]**（仮想トークンの参照）オプションが表示されない	Credential Manager では、セキュリティ リスクを避けるために、参照オプションが削除されたため、ユーザは登録した仮想トークンの位置を移動できません	参照オプションを使用できると、ユーザ以外がファイルの削除や名前の変更を行って Windows を制御できるようになるため、今回の製品からは、参照オプションは削除されています
TPM 認証でログインする場合、**[Network Accounts]**（ネットワーク アカウント）オプションが提供されない	**[Network Accounts]**（ネットワーク アカウント）オプションを使用すると、ログインするドメイン アカウントを選択できます。TPM 認証を使用する場合、このオプションは使用できません	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です

簡単な説明	詳しい説明	解決方法
権限がある場合でも、ドメイン管理者が Windows パスワードを変更できない	これは、ドメイン管理者がドメインにログオンし、ドメインとローカル コンピュータで管理者の権限をもつアカウントを使用して、ドメイン ID を Credential Manager に登録した後で発生します。ドメイン管理者が、Credential Manager から Windows のパスワードを変更しようとすると、ログオンの失敗を示す次のようなエラー メッセージが表示されます。**[User account restriction]**（ユーザ アカウントの制限）	Credential Manager が**[Change Windows password]**（Windows パスワードを変更する）を使用して、ドメイン ユーザのアカウント パスワードを変更することはできません。Credential Manager が変更できるのは、ローカル コンピュータのアカウント パスワードだけです。ドメイン ユーザは、**[Windows security]**（Windows セキュリティ）→**[Change password]**（パスワードを変更する）オプションを使用して自身のパスワードを変更できますが、ドメイン ユーザはローカル コンピュータに実質的なアカウントを持っていないため、Credential Manager が変更できるのはログインに使用するパスワードだけです
Credential Manager シングルサインオンの初期設定を、ループを防止するメッセージを表示するように設定する必要がある	シングルサインオンの初期設定は、ユーザは自動的にログに記録されます。ただし、パスワード保護された 2 つの異なるドキュメントを作成する場合、2 つ目を作成するときに、Credential Manager は、最後に記録されたパスワード、つまり最初のドキュメントのパスワードを使用します	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Corel WordPerfect 12 のパスワード gina に対応していない問題	ユーザが Credential Manager にログインして、WordPerfect でドキュメントを作成し、パスワード保護を使用して保存した場合、Credential Manager は、パスワード gina を手動でも自動でも検出または認識できません	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager が画面の**[Connect]**（接続）ボタンを認識しない	リモート デスクトップ接続（RDP）のシングルサインオン証明書が、**[Connect]**（接続）に設定されている場合でも、再起動時のシングルサインオンでは、常に**[Connect]**（接続）ではなく**[Save as]**（名前を付けて保存）が入力されます	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager と共に ATI Catalyst 設定ウィザードを使用できない	Credential Manager のシングルサインオンは、ATI Catalyst 設定ウィザードと競合します	Credential Manager のシングルサインオンを無効にしてください
TPM 認証を使用してログインすると、画面の**[Back]**（戻る）ボタンが別の認証方式を選択するためのオプションをスキップする	Credential Manager の TPM ログイン認証を使用するユーザが、自身のパスワードを入力する場合、**[Back]**（戻る）ボタンは正常に機能しませんが、Windows のログイン画面はすぐに表示されます	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager がスタンバイ モードから起動しないように設定されている場合でも、スタンバイから起動する	オプションで**[use Credential Manager log on to Windows]**（Credential Manager の Windows へのログオンを使用する）が選択されていない場合でも、システムが S3 サスペンドに入るのを許可してからシステムをサスペンドからウェイクアップすると、Credential Manager の Windows へのログオンが開きます	この場合、管理者パスワードが設定されていないと、Credential Manager が実行するアカウント制限により、ユーザは、Credential Manager を介して Windows にログオンできません ● Java Card またはトークンがない場合、ユーザは、Credential Manager ログインを取り消すことができ、この場合、Microsoft Windows ログインが表示されます。ユーザはこの時点でログインできます ● Java Card またはトークンがある場合、次の回避策をとると、Java Card 挿入時の Credential

簡単な説明	詳しい説明	解決方法
		Manager の起動を有効または無効にすることができます **1.** **[Advanced Settings]**（詳細設定）をクリックします **2.** **[Service & Application]**（サービスおよびアプリケーション）をクリックします **3.** **[Java Cards and Tokens]**（Java Card およびトークン）をクリックします **4.** Java Card/ トークンを挿入したらクリックします **5.** **[Advise to log-on]**（ログオンをアドバイスする）チェックボックスにチェックを入れます
TPM モジュールが取り外されたり破損したりすると、TPM によって保護されていた Credential Manager 証明書がすべて失われる	TPM モジュールが取り外されたり破損したりすると、TPM が保護する証明書がすべて失われます	これは仕様です TPM モジュールは、Credential Manager の証明書を保護するように設計されています。TPM モジュールを取り外す前に、Credential Manager の ID 情報をバックアップすることをおすすめします
Windows 2000 で、Credential Manager がプライマリ ログオンとして設定されない	Windows 2000 のインストール時、ログオン ポリシーは手動または自動のログオンによる管理に設定されます。自動ログオンが選択されている場合、Windows の初期のレジストリ設定では、初期 AutoAdminLogon 値が「1」に設定され、Credential Manager はこの値を無効にしません	これは仕様です バイパスのための AutoAdminLogon 値のオペレーティング システム レベル設定を変更する場合、編集パスは次のとおりです。HKEY_LOCAL_MACHINE/ Software/Microsoft/ WindowsNT/CurrentVersion/ WinLogon **注意：** レジストリ エディタを使用して、ご自身の責任で編集してください。レジストリ エディタ（regedit）の使用法を誤ると、重大な問題が発生して、オペレーティング システムの再インストールが必要になる場合があります。レジストリ エディタの使用法を誤って問題が発生した場合、その問題を解決できる保証はありません
指紋認証システムが設置または登録されているかどうかに関係なく、指紋認証ログオン メッセージが表示される	ユーザが Windows ログオンを選択する場合、Credential Manager のタスク バーに次の警告が表示されます。**[You can place your finger on the fingerprint reader to log on to Credential Manager]（指紋認証システムの上に指を置くと、Credential Manager にログオンできます）**	この警告の目的は、指紋認証が設定されている場合、この認証方式を利用できることをユーザに示すことです
リーダーが接続されていないのに、Windows 2000 用の Credential Manager ログオン ウィンドウに **[insert card]**（カードを挿入してください）と表示される	Java Card リーダーが接続されていない場合でも、Windows の Credential Manager の[Welcome]（ようこそ）画面に **[insert card]**（カードを挿入してください）と表示され、ユーザがカードを挿入してログオンできることが示されます	この警告の目的は、Java Card 認証が設定されている場合、この認証方式を利用できることをユーザに示すことです
Windows XP Service Pack 1（このバージョンのみ）でスリープ モードからハイバネーションに移ると、Credential Manager にログインできなくなる	システムをハイバネーションやスリープ モードに移行できるように設定すると、どのログオン証明書（パスワード、指紋、または Java Card）が選択されている場合でも、管理者またはユーザは Credential Manager にログインできなくなり、Windows のログオン画面が表示されたままになります	この問題は、Microsoft 社の提供する Service Pack 2 で解決されたようです。この問題の原因については、http://www.microsoft.com/japan/で、Microsoft サポート技術情報の記事 813301 を参照してください ログオンするには、Credential Manager を選択してログインする必要があります。Credential Manager にログインすると、ログイン プロセスを完了するために、Windows（Windows ログイン オプションを選択しなければならない場合があります）にログインするように指示されます

簡単な説明	詳しい説明	解決方法
		初めて Windows にログインする場合は、手動で Credential Manager にログインする必要があります
Embedded Security を復元すると、Credential Manager が機能しなくなる	ROM を工場出荷時の設定に復元した後は、Credential Manager が証明書を登録できなくなります	HP Credential Manager for ProtectTools のインストール後、ROM が工場出荷時の設定にリセットされた場合、Credential Managers が TPM にアクセスできなくなります TPM 内蔵セキュリティ チップは、BIOS のコンピュータ セットアップ（F10）ユーティリティ、BIOS Configuration for ProtectTools、または HP Client Manager で有効にできます。TPM 内蔵セキュリティ チップを有効にするには、以下の手順で操作します 1. コンピュータの電源を入れるか再起動し、画面の左下隅に**[F10=ROM Based Setup]**メッセージが表示されている間に F10 キーを押して、コンピュータ セットアップ（F10）ユーティリティを起動します 2. 矢印キーを使用し、**[セキュリティ]**（Security）→**[セットアップ パスワード]**（Setup Password）の順に選択します。パスワードを設定します 3. **[Embedded Security Device]**（内蔵セキュリティ デバイス）を選択します 4. 矢印キーを使用して、**[無効]**（Embedded Security Device–Disable）を選択します。矢印キーを使用して、**[有効]**（Embedded Security Device–Enable）に変更します 5. **[有効]**（Enable）→**[変更を保存して終了]**（Save changes and exit）の順に選択します HP では、将来のカスタマ ソフトウェア リリースに向けて、解決策を調査中です
セキュリティの**[Restore Identity]**（ID の復元）プロセスにより、仮想トークンとの関連付けが失われる	ユーザが ID を復元すると、Credential Manager のログイン画面で仮想トークンの位置との関連付けが失われることがあります。Credential Manager が仮想トークンを登録している場合でも、関連付けを復元するには、ユーザがトークンを再登録する必要があります	現在の仕様です ID を維持しないで Credential Manager をアンインストールすると、ID の復元によりトークンのクライアント部分が復元されても、トークンのシステム（サーバ）部分が壊れ、トークンをログオンに使用できなくなります HP では、一時的ではない解決策を調査中です

Embedded Security for ProtectTools

簡単な説明	詳しい説明	解決方法
PSD でフォルダ、サブ フォルダ、およびファイルを暗号化すると、エラー メッセージが表示される	ファイルとフォルダを PSD にコピーしてフォルダ/ファイルまたはフォルダ/サブフォルダを暗号化しようとすると、**[Error Applying Attributes]**（属性適用時のエラー）メッセージが表示されます。別に取り付けたハードディスク ドライブ上の C:\ドライブで同じファイルを暗号化することはできます	これは仕様です ファイル/フォルダを PSD に移動するとそのファイル/フォルダは自動的に暗号化されます。ファイル/フォルダを二重に暗号化する必要はありません。EFS を使用して PSD のファイル/フォルダを二重に暗号化しようとすると、このエラー メッセージが表示されます
マルチブート プラットフォーム環境で別の OS を使用して所有権を得ることができない	ドライブがマルチ OS ブート用にセットアップされている場合でも、所有権の設定は、1 つのオペレーティング システムのプラットフォーム初期化ウィザードからのみ行えます	これはセキュリティを確保するための仕様です
管理者権限のある不正なユーザが、暗号化された EFS フォルダの内容の表示、削除、名前変更、移動を行える	フォルダを暗号化している場合でも、管理権限がある不正なユーザは、フォルダの内容の表示、削除、または移動を行えます	これは仕様です これは、Embedded Security TPM ではなく EFS の機能です。Embedded Security は、Microsoft EFS ソフトウェアを使用し、EFS がすべての管理者のファイル/フォルダへのアクセス権限を保護します
EFS で暗号化されたフォルダは、Windows 2000 では緑色で強調表示されません	EFS で暗号化されたフォルダは、Windows XP では緑色で強調表示されますが、Windows 2000 ではそのように表示されません	これは仕様です Windows 2000 では暗号化されたフォルダが強調表示されないが、Windows XP では強調表示されるという現象は、EFS の機能です。これは、Embedded Security TPM がインストールされている場合もされていない場合も発生します
Windows 2000 では暗号化されたファイルを表示するときに EFS がパスワードを要求しない	Windows 2000 システムでは、Embedded Security をセットアップして、管理者としてログオンし、いったんログオフしてからもう一度管理者としてログオンすると、パスワードを入力しなくてもファイルとフォルダを表示できます。この状態は Windows 2000 の 1 番目の管理者アカウントで発生します。セカンダリ管理者アカウントでログインした場合、このような状態は発生しません	これは仕様です これは、Windows 2000 の EFS の機能です。Windows XP の EFS の初期設定では、ユーザはパスワードなしでファイル/フォルダを開くことはできません
FAT32 パーティションの復元で、ソフトウェアをインストールできない	FAT32 を使用するハードディスク ドライブを復元する場合は、EFS を使用してファイル/フォルダを暗号化するオプションが表示されません	これは仕様です Microsoft EFS は、NTFS でのみサポートされており、FAT32 では機能しません。これは、Microsoft EFS の機能であり、HP ProtectTools ソフトウェアとは関係ありません
Windows 2000 ユーザは非表示の（$）共有を使用して、任意の PSD をネットワーク経由で共有できる	Windows 2000 ユーザは非表示の（$）共有を使用して、任意の PSD をネットワーク経由で共有できます。非表示共有には、非表示の（$）共有を使用してネットワーク経由でアクセスできます	PSD は、一般的にネットワークでは共有されませんが、Windows 2000 に限り、非表示の（$）共有を使用すると共有できます。このため、ビルトイン アカウントの管理者をパスワードで保護することをおすすめします
ユーザがリカバリ アーカイブ XML ファイルの暗号化または削除を行える	設計では、このフォルダの ACL は設定されていません。このため、意図的かどうかに関係なく、ユーザがこのファイルを暗号化または削除して、アクセスできなくなる可能性があります。ファイルが暗号化または削除されると、TPM ソフトウェアをだれも使用できなくなります	これは仕様です ユーザは、基本ユーザ キーのバックアップ コピーを保存または更新するために、緊急アーカイブにアクセスすることができます。最善のセキュリティ方針を採用し、ユーザがリカバリ アーカイブ ファイルを暗号化または削除しないよう周知徹底する必要があります
HP ProtectTools Embedded Security EFS と Symantec Antivirus または Norton Antivirus 製品	ファイルが暗号化されていると、Symantec Antivirus または Norton Antivirus 2005 のウィルス スキャンが中断されます。スキャン プロセス中、約	HP ProtectTools Embedded Security EFS ファイルのスキャンにかかる時間を短縮するには、スキャンの前に暗号パスワードを入力するか、またはスキャンの前に暗号化を解除します

簡単な説明	詳しい説明	解決方法
とのやり取りで暗号化/暗号化の解除およびスキャンにかかる時間が延びる	10 ファイルごとに、基本ユーザのパスワード プロンプトが表示され、パスワードの入力を求められます。パスワードを入力しなくても、基本ユーザのパスワード プロンプトがタイムアウトするため、Norton Antivirus 2005 はスキャンを続行できます。HP ProtectTools Embedded Security EFS を使用してファイルを暗号化すると、Symantec Antivirus または Norton Antivirus の実行時間が延びます	HP ProtectTools Embedded Security EFS を使用したデータの暗号化/暗号化の解除にかかる時間を短縮するには、Symantec Antivirus または Norton Antivirus の Auto-Protect を無効にする必要があります
リムーバブル メディアに緊急リカバリ アーカイブを保存できない	Embedded Security の初期化中に、緊急リカバリ アーカイブのパスを作成するとき、MMC または SD カードを挿入すると、エラー メッセージが表示されます	これは仕様です リムーバブル メディアにリカバリ アーカイブを保存することはできません。リカバリ アーカイブはネットワーク ドライブまたは C ドライブ以外のローカル ドライブに保存することができます
Windows 2000 のフランス語環境で、データを暗号化できない	ファイル アイコンを右クリックしても、**[Encrypt]**（暗号化）オプションが表示されません	これは、Microsoft オペレーティング システムの制限事項です。[French (Canada)]（フランス語（カナダ））など、他の地域にロケールを変更すると、**[Encrypt]**（暗号化）オプションが表示されます これを回避するには、次の手順でファイルを暗号化します。ファイル アイコンを右クリックし、**[Properties]**（プロパティ）→**[Advanced]**（詳細）→**[Encrypt Contents]**（内容の暗号化）の順に選択します
Embedded Security の初期化中に所有者を設定しているときに電源が切断されるとエラーが発生する	内蔵セキュリティ チップの初期化中に電源が切断されると、次のような問題が発生します ● Embedded Security Initialization Wizard（内蔵セキュリティ初期化ウィザード）の起動を試みると、次のエラー メッセージが表示されます。**[The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.]**（**Embedded Security チップに Embedded Security の所有者がすでに設定されているため、Embedded Security を初期化できません**） ● User Initialization Wizard（ユーザ初期化ウィザード）の起動を試みると、次のエラー メッセージが表示されます。**[The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.]**（内蔵セキュリティが初期化されていません。ウィザードを使用するには、内蔵セキュリティを最初に初期化する必要があります）	電源が切断された後は、以下の手順に沿って回復します **注記：** メニューやメニュー項目の選択および値の変更には、特に指定がない場合は、矢印キーを使用します 1. コンピュータを起動または再起動します 2. 画面に**[F10=Setup]**メッセージが表示されたら（またはモニタのランプが緑色に点灯したらすぐに）F10 キーを押します 3. 該当する言語オプションを選択します 4. Enter キーを押します 5. **[Security]**（セキュリティ設定）→**[Embedded Security]**（内蔵セキュリティ）の順に選択します 6. **[Embedded Security Device]**（内蔵セキュリティ デバイス）オプションを**[Enable]**（有効）に設定します 7. F10 キーを押して、変更を確定します 8. **[ファイル]**→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します 9. Enter キーを押します 10. F10 キーを押して変更を保存し、コンピュータ セットアップ（F10）ユーティリティを終了します
コンピュータ セットアップ（F10）ユーティリティのパスワードは、TPM モ	TPM モジュールを有効にするには、コンピュータ セットアップ（TPM）ユーティリティのパスワードが必要です。モ	これは仕様です

簡単な説明	詳しい説明	解決方法
ジュールを有効にした後で削除できる	ジュールを有効にすると、ユーザはパスワードを削除できます。パスワードを削除すると、システムに直接アクセスするユーザであれば誰でも TPM モジュールをリセットできるため、データ消失の原因になる可能性があります	コンピュータ セットアップ（F10）ユーティリティのパスワードは、パスワードを知っているユーザだけが削除できます。ただし、コンピュータ セットアップ（F10）ユーティリティのパスワードは常に保護しておくことを強くおすすめします
システムがスタンバイ状態からアクティブに切り替わると、PSD のパスワード ボックスが表示されなくなる	PSD の作成後ユーザがシステムにログオンすると、TPM は基本ユーザ パスワードの入力を要求します。ユーザがパスワードを入力しないままシステムがスタンバイ状態になると、ユーザが再開してもパスワード ダイアログ ボックスは表示されません	これは仕様です ユーザがいったんログオフしてからログオンすれば、PSD パスワード ボックスは表示されます
セキュリティ プラットフォーム ポリシーを変更するときに、パスワードを要求されない	セキュリティ プラットフォーム ポリシーへのアクセス（マシンとユーザの両方）では、システムの管理権限を持っているユーザは、TPM パスワードの入力を要求されません	これは仕様です TPM ユーザが初期化されている場合でもされていない場合でも、管理者であればセキュリティ プラットフォーム ポリシーを変更できます
Windows 2000 で Microsoft EFS が完全に機能しない	管理者は、正しいパスワードを知らなくても、システムの暗号化された情報にアクセスできます。管理者が誤ったパスワードを入力した場合やパスワード ダイアログを取り消した場合でも、暗号化されたファイルは正しいパスワードを入力した場合と同じように開きます。この現象は、データを暗号化するときのセキュリティ設定とは関係なく発生します。この状態は Windows 2000 の 1 番目の管理者アカウントで発生します	データ リカバリ ポリシーは、管理者をリカバリ エージェントとして指名するように自動的に設定されます。ユーザ キーを取得できない場合（誤ったパスワードを入力した場合や、[Enter Password]（パスワードの入力）ダイアログを取り消した場合）、ファイルはリカバリ キーを使用して自動的に暗号化が解除されます この原因は、Microsoft EFS にあります。詳しくは、http://www.microsoft.com/japan/で、Microsoft サポート技術情報の記事 Q257705 を参照してください 管理者以外のユーザがこのドキュメントを開くことはできません
証明書を表示すると、信頼されていないものとして表示される	HP ProtectTools をセットアップして User Initialization Wizard（ユーザ初期化ウィザード）を実行した後、ユーザは発行された証明書を表示できますが、その証明書は信頼されていないものとして表示されます。ここで、インストール ボタンをクリックして証明書をインストールすることはできますが、インストールしても、信頼済みに変わることはありません	自己署名の証明書は、信頼されません。正しく設定された企業環境では、EFS の証明書は、オンラインの証明機関が発行し、信頼されます
次の暗号化/暗号化の解除エラーが断続的に発生する。**[The process cannot access the file because it is being used by another process.]（ファイルが別のプロセスによって使用されているため、このプロセスはファイルにアクセスできません）**	ファイルの暗号化または暗号化の解除中に、ファイルが別のプロセスによって使用されていることが原因のエラーがきわめて断続的に発生します。これは、該当するファイルまたはフォルダがオペレーティング システムまたはその他のアプリケーションで処理されていない場合でも発生します	この問題を解決するには、次の手順で操作します 1. システムを再起動します 2. ログオフします 3. 再度ログインします
新しいデータ生成または転送の前にストレージを取り外すと、リムーバブル ストレージでデータが消失する	マルチベイ ハードディスク ドライブなどストレージ メディアを取り外しても、PSD が使用可能と表示され、PSD のデータを追加または変更するときにエラーが生成されません。システムの再起動後、リムーバブル ストレージが使用できなかった期間にファイルに加えられた変更箇所は、PSD に反映されません	この問題は、ユーザが PSD にアクセスした後、新しいデータの生成または転送が完了する前に、ハードディスク ドライブを取り外した場合にのみ発生します。リムーバブル ハードディスク ドライブが存在しないときに PSD にアクセスすると、**[the device is not ready]**（デバイスの準備ができていません）というエラー メッセージが表示されます

簡単な説明	詳しい説明	解決方法
基本ユーザの初期化が行われていない場合、アンインストールのために管理ツールを開くと、**[Disable]**（無効）オプションが使用できず、アンインストーラは管理ツールを閉じるまで作業を停止する	ユーザは TPM を無効にしないでアンインストールを行うか、または最初に TPM を無効にして（管理ツールを使用）からアンインストールを行うかを選択できます。管理ツールにアクセスするには、基本ユーザ キーを初期化する必要があります。基本ユーザ キーを初期化していない場合、ユーザはどのオプションにもアクセスできません ユーザは、**[Click Yes to open Embedded Security Administration tool]**（Embedded Security 管理ツールを開くには、[Yes]（はい）をクリックします）と指示するダイアログ ボックスで**[Yes]**（はい）をクリックして明示的に管理ツールを開くことを選択しているため、管理ツールが閉じられるまでアンインストールは実行されません。ダイアログ ボックスで、**[No]**（いいえ）をクリックすると、管理ツールが開かないため、アンインストールは実行されます	TPM チップを無効にするには、管理ツールを使用しますが、基本ユーザ キーを初期化していない場合は、そのためのオプションは使用できません。基本ユーザ キーを初期化していない場合にアンインストール プロセスを続行するには、**[OK]**または**[Cancel]**（キャンセル）を選択してください
128 MB のシステム構成で、2 つのユーザ アカウントで PSD を作成し、高速ユーザ切り替えを使用すると、システムが断続的にロックする	RAM の容量がきわめて少ない状態で高速切り替えを行うと、システムがロックすることがあります。このとき[ようこそ（ログオン)]画面が表示されず、画面が黒色になり、キーボードとマウスを操作しても応答はありません	メモリ容量の少ない構成で発生するタイミングの問題が、根本原因になっていると思われます 内蔵グラフィックスが UMA アーキテクチャを使用するために 8 MB のメモリが使用され、ユーザ領域として 120 MB だけ残ります。エラーが発生した状況では、2 人のユーザがログインし高速でユーザの切り替えを行っています。エラーの発生時には、120 MB のメモリがこの 2 人のユーザで共有されています この問題を回避するには、システムを再起動します。また、メモリを増設することをおすすめします（セキュリティ モジュールを搭載し、メモリの初期設定時の構成が 128 MB のシステムは販売されていません）
[access denied]（アクセスが拒否されました）というメッセージが表示され、EFS ユーザ認証（パスワード要求）がタイムアウトする	**[OK]**をクリックするか、タイムアウト後にスタンバイ状態から復帰すると、EFS ユーザ認証パスワードが再度開きます	これは仕様です。Microsoft EFS で問題が発生しないように、エラー メッセージを生成するために 30 秒程度のウォッチドッグ タイマーが作成されました
日本語のセットアップ時に、機能説明の一部が省略される	インストール ウィザード実行時のカスタム セットアップ オプション段階で、機能説明が省略されています	この問題については、将来のリリースで解決します
プロンプトでパスワードを入力しなくても EFS 暗号化が行われる	ユーザ パスワードのプロンプトのタイムアウトが許可されており、タイムアウトが発生した場合でも、ファイルまたはフォルダを暗号化できます	暗号化は Microsoft EFS 暗号化の機能のため、暗号化にパスワード認証は不要です。暗号化を解除する場合は、ユーザ パスワードを入力する必要があります
User Initialization Wizard（ユーザ初期化ウィザード）でチェックを外している場合やユーザ ポリシーでセキュリティ保護された電子メールの設定を無効にしている場合でも、セキュリティ保護された電子メールがサポートされる	Embedded Security ソフトウェアとそのウィザードは、電子メール クライアント（Outlook、Outlook Express、または Netscape）の設定を制御しません	この動作は仕様です。TPM の電子メール設定では、電子メールクライアントの暗号化設定を直接編集することを禁じていません。セキュリティ保護された電子メールの使用は、他社製のアプリケーションが設定し、制御します。HP のウィザードでは、即座にカスタマイズを行う 3 つの参照アプリケーションを関連付けることができます
同じコンピュータまたは以前に初期化したコンピュータで 2 回目の大規	以前に初期化した HP ProtectTools Embedded Security システムで大規模な導入を実行すると、既存のリカバリ アー	HP では、この xml ファイルの上書きの問題の解決に向けて取り組みを進めており、将来の SoftPaq で解決策が提供される予定です

簡単な説明	詳しい説明	解決方法
模な導入を実行すると、緊急リカバリ ファイルおよび緊急トークン ファイルが上書きされる。新しいファイルは、リカバリに使用できない	カイブ xml ファイルとリカバリ トークン xml ファイルが上書きされ、使用できなくなります	
Embedded Security でユーザの復元を実行中に、自動ログオン スクリプトが機能しない	ユーザが次の操作を行った後、エラーが発生します ● Embedded Security で、所有者とユーザを初期化する（初期設定時の位置の**[マイ ドキュメント]**を使用） ● BIOS で、チップを工場出荷時の設定に戻す ● コンピュータを再起動する ● Embedded Security の復元を開始する。復元プロセス中、Credential Manager は、システムが Infineon TPM User Authentication へのログオンを自動化できるかどうかをユーザにたずねます。ユーザが**[Yes]**（はい）を選択すると、テキスト ボックスに SPEmRecToken の位置が自動的に表示されます この位置が正しい場合でも、次のエラー メッセージが表示されます。**[No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.]**（緊急リカバリ トークンが入力されていません。緊急リカバリ トークンの取得元にするトークン位置を選択してください。）	画面の**[Browse]**（参照）ボタンをクリックして位置を選択してください。復元プロセスが続行されます
高速ユーザ切り替え環境で、複数ユーザ PSD が機能しない	複数のユーザが作成され、PSD に同じドライブ文字が割り当てられると、この問題が発生します。PSD がロードされているとき、ユーザを高速で切り替えようとすると、2 番目のユーザの PSD を使用できなくなります	2 番目のユーザの PSD を使用するには、別のドライブ文字を使用するように設定し直すか、または最初のユーザがログオフする必要があります
PSD を作成したハードディスク ドライブをフォーマットすると、PSD が無効になり、削除できなくなる	PSD を作成したセカンダリ ハードディスク ドライブをフォーマットすると、PSD が無効になり、削除できなくなります。PSD のアイコンは残りますが、PSD へのアクセスを試みると、**[drive is not accessible]**（ドライブにアクセスできません）というエラー メッセージが表示されます PSD を削除することはできません。次のようなメッセージが表示されます。**[your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process.]**（PSD は使用中です。PSD 上のファイルが開かれていないことと別のプロセスでアクセスされていないことを確認してください） PSD を削除するには、システムを再起動する必要があります。再起動後、PSD はロードされません	これは仕様です。ユーザが強制的に削除したり、PSD データの保存位置から切断したりしても、Embedded Security PSD ドライブ エミュレーションが機能を続行し、存在しないデータとの通信が途切れるため、エラーが生成されます 解決策：次の再起動後はエミュレーションがロードされないため、ユーザは古い PSD エミュレーションを削除して、新しい PSD を作成できます

簡単な説明	詳しい説明	解決方法
自動バックアップ アーカイブからの復元時に、内部エラーが検出された	ユーザが次の操作を行うと問題が発生します • HPPTSM で、[Embedded Security]（内蔵セキュリティ）の **[Restore under Backup]**（バックアップに基づいて復元する）オプションをクリックして、自動バックアップ アーカイブから復元しようとする • **[SPSystemBackup.xml]**を選択する Restore Wizard（復元ウィザード）が機能しなくなり、次のエラー メッセージが表示されます。**[The selected Backup Archive does not match the restore reason. Please select another archive and continue.]**（選択したバックアップ アーカイブは復元理由にふさわしくありません。別のアーカイブを選択して続行してください）	SpBackupArchive.xml が必要な場合にユーザが **[SpSystemBackup.xml]**を選択すると、次のメッセージが表示されて Embedded Security Wizard（Embedded Security ウィザード）が機能しなくなります。**[An internal Embedded Security error has been detected]**（**Embedded Security 内部エラーが検出されました**） 所定の理由に該当する、正しい.xml ファイルを選択する必要があります プロセスは設計どおりに正しく機能していますが、Embedded Security 内部エラー メッセージが明確でないため、より適切なメッセージを表示する必要があります。HP は、将来の製品で改善するよう取り組んでいます
セキュリティ システムにより、複数のユーザでの復元エラーと表示される	復元プロセス中、管理者が復元するユーザを選択した場合、選択されなかったユーザが後で復元を試みてもキーを復元できません。**[decryption process failed]**（暗号化の解除プロセスが失敗しました）というエラー メッセージが表示されます	選択されなかったユーザは、次の初期設定の日常バックアップが実行される前に、TPM をリセットして、復元プロセスを実行し、すべてのユーザを選択すれば、復元できます。自動バックアップが実行されると、復元されていないユーザは上書きされ、そのデータは失われます。新しいシステム バックアップが保存されると、選択されていない以前のユーザを復元することはできなくなります また、ユーザはシステム バックアップ全体を復元する必要があります。アーカイブ バックアップは、個別に復元できます
システム ROM を初期設定に戻すと、TPM を認識できなくなる	システム ROM を初期設定に戻すと、Windows が TPM を認識できなくなります。これより、セキュリティ ソフトウェアが正しく動作しなくなり、TPM の暗号化データにアクセスできなくなります	以下の手順に従って、BIOS で TPM を再表示します コンピュータ セットアップ（F10）ユーティリティを開き、**[Security]**（セキュリティ）→**[Device security]**（デバイス セキュリティ）の順に選択し、フィールドを**[Hidden]**（非表示）から**[Available]**（使用可能）に変更します
マップされたドライブで自動バックアップが機能しない	管理者が Embedded Security で自動バックアップをセットアップすると、**[Windows]**→**[Tasks]**→**[スケジュールされたタスク]**にエントリが作成されます。この Windows の[スケジュールされたタスク]は、バックアップ実行権限用に NT AUTHORITY\SYSTEM を使用するように設定されます。この設定は、どのローカル ドライブに対しても有効に機能します 管理者が、自動バックアップでマップされたドライブに保存されるように設定すると、NT AUTHORITY\SYSTEM にはマップされたドライブを使用する権限がないため、プロセスは失敗します ログイン時に自動バックアップが行われるようにスケジュール設定されている場合、Embedded Security の TNA アイコンに次のメッセージが表示されます。**[The Backup Archive location is currently not accessible. Click here if**	この問題を回避するには、NT AUTHORITY\SYSTEM を[コンピュータ名]\[管理者名]に変更してください。これは、スケジュールされたタスクが手動で作成される場合の初期設定です HP では、[コンピュータ名]\[管理者名]を含む初期設定を備える製品を将来リリースできるよう取り組みを進めています

簡単な説明	詳しい説明	解決方法
	you want to backup to a temporary archive until the Backup Archive is accessible again.]（現在、バックアップ アーカイブの位置にアクセスできません。バックアップ アーカイブにアクセスできるようになるまで、一時的なアーカイブにバックアップする場合は、ここをクリックしてください） ただし、自動バックアップが特定の時間に実行されるように設定されている場合、バックアップは失敗し、失敗を示すメッセージは表示されません	
Embedded Security GUI で、Embedded Security の状態を一時的に無効にすることができない	最新の 4.0 ソフトウェアは、HP Notebook 1.1B への実装と、HP Desktop 1.2 への実装をサポートすることを目的にして設計されました 無効化のためのこのオプションは、TPM 1.1 プラットフォームのソフトウェア インタフェースでもサポートされています	この問題については、将来のリリースで対応します

その他

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
HP ProtectTools Security Manager で次の警告が表示される。**[The security application can not be installed until the HP Protect Tools Security Manager is installed]**（HP ProtectTools セキュリティ マネージャをインストールするまでは、セキュリティ アプリケーションをインストールできません）	Embedded Security、Java Card、指紋認証などのセキュリティ アプリケーションは、すべて HP セキュリティ マネージャ インタフェースの拡張プラグインです。セキュリティ マネージャがインストールされていないと、HP 認定のセキュリティ プラグインをロードすることはできません	セキュリティ プラグインをインストールする前に、HP ProtectTools セキュリティ マネージャ ソフトウェアをインストールする必要があります
dc7600 や Broadcom 対応 TPM を搭載したモデル用の HP ProtectTools TPM Firmware Update Utility：HP のサポート Web サイトを通じて提供されるこのツールで **[ownership required]**（所有権が必要です）と報告される	これは、dc7600 や Broadcom 対応 TPM を搭載したモデル用の TPM ファームウェア ユーティリティで想定された動作です ユーザは、公認キー（EK）がある場合もない場合も、このファームウェア アップグレード ツールを使用して、ファームウェアをアップグレードできます。EK がない場合は、ファームウェア アップグレードの実行に権限は必要ありません EK がある場合は、アップグレードに所有者の権限が必要なため、TPM 所有者が存在する必要があります。アップグレードが正常に行われた後、プラットフォームを再起動して、新しいファームウェアを有効にする必要があります BIOS TPM が工場出荷時の状態にリセットされると、所有権は削除され、Embedded Security ソフトウェアのプラットフォームとユーザの初期化のためのウィザードの設定が完了するまで、アップデート機能を使用できません *ファームウェア アップデートの実行後に必ずシステムを再起動することをおすすめします。ファームウェア バージョンは、再起動が完了するまでは正しく識別されません	1. HP ProtectTools Embedded Security ソフトウェアを再インストールします 2. プラットフォームおよびユーザの設定ウィザードを実行します 3. 以下の手順に従って、システムに Microsoft. NET framework 1.1 がインストールされていることを確認します a. **[スタート]**をクリックします b. **[コントロール パネル]**をクリックします c. **[プログラムの追加と削除]**をクリックします d. **[Microsoft .NET Framework 1.1]**があることを確認します 4. 以下の手順に従って、ハードウェアとソフトウェアの構成を確認します a. **[スタート]**をクリックします b. **[すべてのプログラム]**をクリックします c. **[HP ProtectTools セキュリティ マネージャ]**をクリックします d. ツリー メニューから**[Embedded Security]**（内蔵セキュリティ）を選択します e. **[More Details]**（詳細）をクリックします システムは、次のような構成になっている必要があります • Product version（製品バージョン）= V4.0.1 • Embedded Security State（内蔵セキュリティの状態）: Chip State（チップの状態）＝ Enabled（有効）、Owner State（所有者の状態）＝ Initialized（初期化済み）、User State（ユーザの状態）＝ Initialized（初期化済み） • Component Info（コンポーネント情報）: TCG Spec. Version（TCG 仕様バージョン）= 1.2

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
		● Vendor（ベンダ） = Broadcom Corporation ● FW Version（FW バージョン） = 2.18（または、それ以上） ● TPM デバイス ドライバ ライブラリ バージョン 2.0.0.9（またはそれ以上） 5. [FW Version]（iFW バージョン）が「2.18」になっていない場合は、TPM ファームウェアをダウンロードして更新してください。TPM ファームウェア SoftPaq は、http://www.hp.com/jp/からダウンロードできます
HP ProtectTools セキュリティ マネージャ：セキュリティ マネージャ インタフェースを閉じたとき、エラーが返されることがある	すべてのプラグイン アプリケーションのロードが終了する前に、セキュリティ マネージャを閉じようとして画面右上の閉じるボタンを使用すると、エラーが発生することがあります（12 回に 1 回ぐらいの割合）	これは、セキュリティ マネージャを終了および再起動するときに、そのタイミングがプラグイン サービス ロード時間の影響を受けることに関連しています。PTHOST.exe は、他のアプリケーション（プラグイン）を収納するシェルであるため、プラグインのロード時間（サービス）の終了能力の影響を受けます。この問題の根本原因は、プラグインのロード終了にかかる時間が経過していないのにシェルが閉じられたことです セキュリティ マネージャがサービス ロード メッセージ（セキュリティ マネージャ ウィンドウの上部に表示されます）を完了し、すべてのプラグインが左の列に表示されるまで待ちます。障害の発生を防止するために、これらのプラグインがロードされるまでしばらく待ってください
HP ProtectTools *全般：アクセスが制限されていないことや管理者権限が制御されないことが、セキュリティ リスクにつながる	クライアント コンピュータに対するアクセスが制限されていないため、次のような、さまざまなリスクが発生します ● PSD の削除 ● ユーザ設定の意図的な改ざん ● セキュリティ ポリシーやセキュリティ機能の無効化	管理者が最善の方法でエンドユーザの権限を制限し、ユーザのアクセスを制限することをおすすめします 不正なユーザに管理権限を与えないでください
BIOS と OS の Embedded Security パスワードが同期していない	ユーザが新しいパスワードを BIOS の Embedded Security パスワードとして有効にしなかった場合、BIOS の Embedded Security パスワードは、コンピュータ セットアップ（F10）ユーティリティの BIOS 設定を通じて、元の Embedded Security パスワードに戻ります	これは仕様です。このパスワードは、OS の基本ユーザ パスワードを変更し、BIOS Embedded Security パスワードのプロンプト画面で認証すれば、再同期されます
BIOS の TPM ブート前認証を有効にした後、1 人のユーザしかシステムにログオンできない	TPM BIOS PIN は、ユーザ設定の初期化を初めて行ったユーザに関連付けられています。コンピュータを複数のユーザで利用する場合、基本的に 1 番目のユーザが管理者になります。1 番目のユーザは、ログインに使用する自分の TPM ユーザ PIN を他のユーザに教える必要があります	これは仕様です。ユーザの IT 部門が適切なセキュリティ ポリシーに従ってセキュリティ ソリューションを展開すること、さらに BIOS 管理者パスワードはシステム レベルで保護されるように必ず IT 管理者が設定することをおすすめします
TPM を工場出荷時設定にリセットした後、TPM 起動前ブートを機能させるためにユーザが PIN を変更しなければならない	TPM のリセット後に TPM BIOS 認証を機能させるため、ユーザは PIN を変更するか、または別のユーザを作成してユーザ自身の設定を初期化する必要があります。他に TPM BIOS 認証を機能させる方法はありません	これは仕様です。工場出荷時の設定にリセットすると基本ユーザ キーは消去されます。ユーザは PIN を変更するか、または別のユーザを作成して基本ユーザ キーを再初期化する必要があります

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
Embedded Security の **[Reset to Factory Settings]**（工場出荷時の設定に戻します）を使用しても、**[Power-on authentication support]**（起動時の認証サポート）が初期設定に戻らない	コンピュータ セットアップ（F10）ユーティリティで、Embedded Security デバイス オプションの**[Reset to Factory Settings]**（工場出荷時の設定に戻します）を使用しても、**[起動時の認証サポート]**オプションは工場出荷時の設定にリセットされません。初期設定では、**[Power-on authentication support]**（起動時の認証サポート）は、**[Disable]**（無効）に設定されます	**[Reset to Factory Settings]**（工場出荷時の設定に戻します）オプションを使用すると、Embedded Security デバイスは無効になり、他の Embedded Security オプション（**[Power-on authentication support]**など）も認識されなくなります。ただし、Embedded Security デバイスを再度有効にすると、**[Power-on authentication support]**は有効のままになります HP では解決策に向けた取り組みを進めており、将来の Web ベース ROM の SoftPaq で提供する予定です
起動シーケンスの実行中に、セキュリティの起動時の認証が BIOS のパスワードと重なる	起動時の認証では、ユーザは TPM パスワードを使用してシステムにログオンすることが求められますが、ユーザが[F10]キーを押して BIOS にアクセスする場合は読み込み権限だけが与えられます	BIOS に書き込みできるようにするには、ユーザは、[Power-on Authentication]（起動時の認証）ウィンドウで TPM パスワードではなく BIOS パスワードを入力する必要があります
Embedded Security Windows ソフトウェアで所有者のパスワードを変更した後に、BIOS がコンピュータ セットアップ（F10）ユーティリティを通じて新旧両方のパスワードを要求する	Embedded Security Windows ソフトウェアで所有者のパスワードを変更した後に、BIOS はコンピュータ セットアップ（F10）ユーティリティを通じて新旧両方のパスワードを要求します	これは仕様です。これは、オペレーティング システムが起動されると、BIOS は TPM と通信できず、TPM パス フレーズを TPM キーの blob と照合できないためです

用語集

BIOS セキュリティ モード　有効にすると、ユーザ認証に Java Card および有効な PIN の使用が必要になる、Java Card セキュリティでの設定。

BIOS プロファイル　他のアカウントに保存および適用できる、BIOS 設定値の集合。

DriveLock　ハードディスク ドライブをユーザにリンクして、コンピュータの起動時にユーザに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

FAT パーティション　ファイル アロケーション テーブル。記憶メディアの索引付けに使用されます。

ID　HP ProtectTools Credential Manager 内で、特定のユーザのアカウントまたはプロファイルのように処理される、証明情報と設定の集合。

Java Card　所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピュータに対して認証するために使用されます。

NTFS パーティション　NT ファイルシステム。記憶メディアの索引付けに使用されます。NTFS は、Windows Vista および Windows XP での標準です。

PSD（Personal Secure Drive）　機密情報を保護するための記憶領域を提供する機能。

TPM（Trusted Platform Module）内蔵セキュリティ チップ（一部のモデルのみ）　機密性の高いユーザ情報を悪意のある攻撃者から保護できる、統合されたセキュリティ チップ。特定のプラットフォーム上の信頼性の基盤です。TPM によって、TCG（Trusted Computing Group）仕様に適合する暗号化アルゴリズムおよび演算方法が提供されます。

USB トークン　ユーザに関する識別情報が格納されているセキュリティ デバイス。Java Card や指紋認証システムと同様に、所有者をコンピュータに対して認証するために使用されます。

Windows ユーザ アカウント　ネットワークまたは個別のコンピュータへのログオンを承認された個人のプロファイル。

暗号化サービス プロバイダ（CSP）　明確なインタフェースを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除　暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）　選択されたフォルダ内のすべてのファイルおよびサブフォルダを暗号化するシステム。

暗号化　権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号法　特定の個人だけが解読できるように、データを暗号化および暗号化解除する手法。

移行　キーおよび証明情報を管理、復元、および転送する作業。

仮想トークン　Java Card やカード リーダーとよく似た働きをするセキュリティ機能。このトークンは、コンピュータのハードディスク ドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

緊急リカバリ アーカイブ　他のプラットフォームの所有者キーを使用して基本ユーザ キーを再暗号化できる、保護された記憶領域。

厳重なセキュリティ　電源投入時パスワード、管理者パスワード、およびその他の形態の、電源投入時認証に対する保護機能を強化する、BIOS Configuration にあるセキュリティ機能。

公開キー基盤（PKI）　証明情報および暗号化キーを作成、使用、および管理するためのインタフェースを定義する規格。

証明書　ユーザが認証プロセスで特定のタスクに対する適格性を証明するための方法。

シングルサインオン　認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに Credential Manager を使用してアクセスできるようにする機能。

スマート カード　所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピュータに対して認証するために使用されます。

デジタル証明書　デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

デジタル署名　資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

電源投入時認証　Java Card、セキュリティ チップ、パスワードなど、コンピュータの起動時に何らかの形式の認証を要求するセキュリティ機能。

ドメイン　ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピュータの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

認証機関　公開キー基盤の運営に必要な証明書を発行するサービス。

認証　ユーザがタスクの実行（たとえば、コンピュータへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

ネットワーク アカウント　ローカル コンピュータ上、ワークグループ内、またはドメイン上の Windows ユーザまたは管理者のアカウント。

バイオメトリック（生体認証）　指紋などの身体的な特徴を使用してユーザを識別する認証証明のカテゴリ。

リブート　コンピュータを再起動するプロセス。

索引